

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-008622  
(43)Date of publication of application : 10.01.2003

(51)Int.Cl. H04L 12/56  
G06F 13/00

(21)Application number : 2001-189497  
(22)Date of filing : 22.06.2001

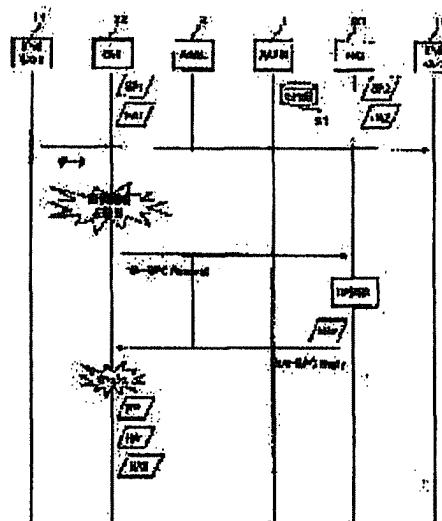
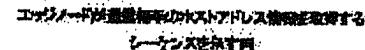
(71)Applicant : FUJITSU LTD  
(72)Inventor : KAKEMIZU MITSUAKI  
MURATA KAZUNORI  
IWAMOTO KATSUNORI  
YAMAMURA SHINYA  
IGARASHI YOICHIRO  
WAKAMOTO MASAAKI

(54) SERVICE CONTROL NETWORK, AND ROUTER EQUIPMENT USED IN THE SERVICE CONTROL NETWORK

**(57)Abstract:**

**PROBLEM TO BE SOLVED:** To efficiently provide services specified for each subscriber or each terminal equipment in a network accommodating a large number of subscribers.

**SOLUTION:** An edge node 22 accommodating an IPv6 host 11 holds service information of the IPv6 host 11 received from an AAA server 1 and host address information of the IPv6 host 11. An edge node 21 accommodating the IPv6 host 12 holds host address information of the IPv6 host 12. The edge node 22 gets the host address information of the IPv6 host 12 from the edge node 21 when a communication from the IPv6 host 11 to the IPv6 host 12 starts. The edge node 22 makes the service information effective using the host address information of the IPv6 hosts 11 and 12 and provides corresponding services.



## LEGAL STATUS

**[Date of request for examination]** 22.03.2007

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

**[Number of appeal against examiner's decision of rejection]**

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (JP)

## (12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-8622

(P2003-8622A)

(43)公開日 平成15年1月10日 (2003.1.10)

(51)Int.Cl.<sup>7</sup>

H 04 L 12/56

G 06 F 13/00

識別記号

3 5 3

F I

H 04 L 12/56

G 06 F 13/00

ジマコート(参考)

Z 5 B 0 8 9

3 5 3 V 5 K 0 3 0

審査請求 未請求 請求項の数10 O L (全 81 頁)

(21)出願番号

特願2001-189497(P2001-189497)

(22)出願日

平成13年6月22日 (2001.6.22)

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番  
1号

(72)発明者 排水 光明

神奈川県川崎市中原区上小田中4丁目1番  
1号 富士通株式会社内

(74)代理人 100074099

弁理士 大曾 義之 (外1名)

最終頁に続く

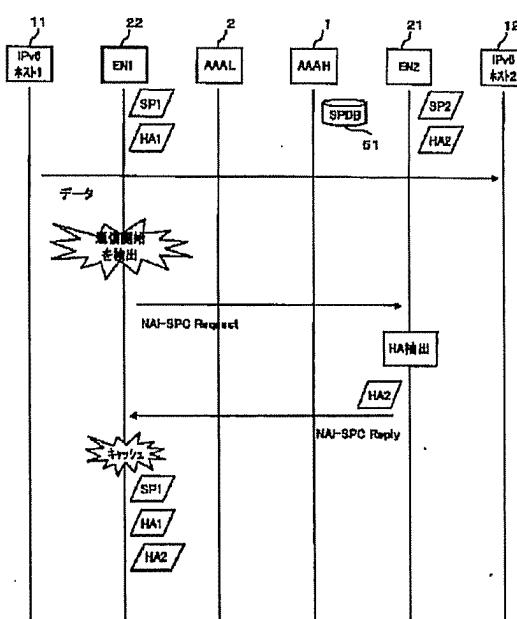
(54)【発明の名称】 サービス制御ネットワーク、及びそのサービス制御ネットワークにおいて使用されるルータ装置

(57)【要約】

【課題】 多数の加入者を収容するネットワークにおいて、加入者ごとまたは端末装置ごとに規定されるサービスを効率的に提供する。

【解決手段】 I Pv 6 ホスト 1 1 を収容するエッジノード 2 2 は、A A A サーバ 1 から受信した I Pv 6 ホスト 1 1 のサービス情報、および I Pv 6 ホスト 1 1 のホストアドレス情報を保持している。I Pv 6 ホスト 1 2 を収容するエッジノード 2 1 は、I Pv 6 ホスト 1 2 のホストアドレス情報を保持している。エッジノード 2 2 は、I Pv 6 ホスト 1 1 から I Pv 6 ホスト 1 2 への通信が開始されたときに、エッジノード 2 1 から I Pv 6 ホスト 1 2 のホストアドレス情報を取得する。エッジノード 2 2 は、I Pv 6 ホスト 1 1 、1 2 のホストアドレス情報を利用してサービス情報を有効化し、対応するサービスを提供する。

エッジノードが通信相手のホストアドレス情報を取得する  
シーケンスを示す図



1

2

## 【特許請求の範囲】

【請求項 1】 端末装置を収容するルータ装置および上記端末装置を認証するサーバ装置を備え、上記端末装置に対してサービスを提供するサービス制御ネットワークであって、

上記ルータ装置は、

上記端末装置からアドレス要求を受信したときに、上記サーバ装置に対して認証要求を送出する要求手段と、上記サーバ装置から上記認証要求に対応する認証応答および上記端末装置のサービス情報を受信し、そのサービス情報に従ってサービスを提供する提供手段と、

上記端末装置に対して上記アドレス要求に対応するアドレス応答を送出する応答手段とを有し、

上記サーバ装置は、上記認証要求に基づいて上記端末装置を認証し、上記認証要求に対応する認証応答および上記端末装置のサービス情報を上記ルータ装置へ送出する送出手段を有することを特徴とするサービス制御ネットワーク。

【請求項 2】 端末装置を収容するルータ装置および上記端末装置を認証するサーバ装置を備え、上記端末装置に対してサービスを提供するサービス制御ネットワークであって、

上記ルータ装置は、

上記端末装置から ICMPv6 によるアドレス要求を受信したときに、上記サーバ装置に対して AAA プロトコルによる認証要求を送出する要求手段と、

上記サーバ装置から上記認証要求に対応する認証応答および上記端末装置のサービス情報を受信し、そのサービス情報に従ってサービスを提供する提供手段と、

上記端末装置に対して上記アドレス要求に対応するアドレス応答を送出する応答手段とを有し、

上記サーバ装置は、上記認証要求に基づいて上記端末装置を認証し、上記認証要求に対応する認証応答および上記端末装置のサービス情報を上記ルータ装置へ送出する送出手段を有することを特徴とするサービス制御ネットワーク。

【請求項 3】 第 1 の端末装置を収容する第 1 のルータ装置、第 2 の端末装置を収容する第 2 のルータ装置、および上記第 1 および第 2 の端末装置に提供すべきサービスを規定するサービス情報を管理するサーバ装置を備え、上記第 1 および第 2 の端末装置にサービスを提供するサービス制御ネットワークであって、

上記第 1 のルータ装置に設けられ、上記第 1 の端末装置に提供すべきサービスを規定するサービス情報を上記サーバ装置から受信して保持する第 1 のサービス情報保持手段と、

上記第 1 のルータ装置に設けられ、上記第 1 の端末装置に設定されているネットワークアクセス識別子と上記第 1 の端末装置に動的に割り当てるアドレスとの対応関係を表すアドレス情報を保持する第 1 のアドレス情報

10

20

30

40

50

保持手段と、

上記第 2 のルータ装置に設けられ、上記第 2 の端末装置に提供すべきサービスを規定するサービス情報を上記サーバ装置から受信して保持する第 2 のサービス情報保持手段と、

上記第 2 のルータ装置に設けられ、上記第 2 の端末装置に設定されているネットワークアクセス識別子と上記第 2 の端末装置に動的に割り当てるアドレスとの対応関係を表すアドレス情報を保持する第 2 のアドレス情報保持手段と、

上記第 1 の端末装置と上記第 2 の端末装置との間の通信を開始した後に、上記第 1 のルータ装置と上記第 2 のルータ装置との間で対応するアドレス情報、あるいはアドレス情報とサービス情報を転送する転送手段と、

上記第 1 のサービス情報保持手段に保持されているサービス情報、上記第 2 のサービス情報保持手段に保持されているサービス情報、上記第 1 のアドレス情報保持手段に保持されているアドレス情報、上記第 2 のアドレス情報保持手段に保持されているアドレス情報、および上記転送手段により転送された情報の少なくとも一部を利用してサービスを提供する提供手段と、

を有することを特徴とするサービス制御ネットワーク。

【請求項 4】 請求項 3 に記載のサービス制御ネットワークであって、

上記サービス情報は、それぞれ対応する端末装置のネットワークアクセス識別子を利用して管理されている。

【請求項 5】 請求項 4 に記載のサービス制御ネットワークであって、

上記第 1 の端末装置から上記第 2 の端末装置へパケットが送出されたときに、上記第 1 および第 2 のアドレス情報保持手段のうちの少なくとも一方により保持されているアドレス情報をを利用して、上記パケットの送信側アドレスおよび受信側アドレスに対応するネットワークアクセス識別子を検出し、その検出されたネットワークアクセス識別子に対応するサービス情報を利用してサービスが提供される。

【請求項 6】 請求項 4 に記載のサービス制御ネットワークであって、

上記第 1 のルータ装置は、

受信したパケットの送信側アドレスおよび受信側アドレスを個別にあるいは組合せで管理するアドレスキャッシュと、

新たに受信したパケットの送信側アドレスまたは受信側アドレスが上記アドレスキャッシュに格納されていなかった場合に、対応するサービス情報を有効化する手段とを有する。

【請求項 7】 請求項 4 に記載のサービス制御ネットワークであって、

上記第 1 のルータ装置は、

受信したパケットの送信側アドレスおよび受信側アドレ

3

スのライフタイムを個別に管理するアドレスキャッシュと、上記アドレスキャッシュにより管理されているアドレスのライフタイムが消滅したときに、対応するアドレス情報およびサービス情報を削除または無効化する手段とを有する。

【請求項8】 第1の端末装置を収容する第1のルータ装置、第2の端末装置を収容する第2のルータ装置、および上記第1および第2の端末装置に提供すべきサービスを規定するサービス情報を管理するサーバ装置を備えるサービス制御ネットワークにおいて、上記第1のルータ装置として使用されるルータ装置であって、上記第1の端末装置に提供すべきサービスを規定するサービス情報を上記サーバ装置から受信し、上記第1の端末装置に設定されているネットワークアクセス識別子と関連づけてそのサービス情報を保持するサービス情報保持手段と、

上記第1の端末装置のネットワークアクセス識別子と上記第1の端末装置に動的に割り当てるアドレスとの対応関係を表すアドレス情報を保持するアドレス情報保持手段と、

上記第1の端末装置から上記第2の端末装置へパケットが送出されたときに、上記アドレス情報保持手段から上記パケットの送信側アドレスに対応するネットワークアクセス識別子を検出し、その検出されたネットワークアクセス識別子に対応するサービス情報を上記サービス情報保持手段から抽出して有効化する有効化手段と、有効化されたサービス情報に従ってサービスを提供する提供手段と、

を有することを特徴とするルータ装置。

【請求項9】 第1の端末装置を収容する第1のルータ装置、第2の端末装置を収容する第2のルータ装置、および上記第1および第2の端末装置に提供すべきサービスを規定するサービス情報を管理するサーバ装置を備えるサービス制御ネットワークにおいて、上記第1のルータ装置として使用されるルータ装置であって、

上記第1の端末装置に提供すべきサービスを規定するサービス情報および上記第2の端末装置に提供すべきサービスを規定するサービス情報を、それぞれ上記第1の端末装置および上記第2の端末装置に設定されているネットワークアクセス識別子と関連づけて保持するサービス情報保持手段と、

上記第1の端末装置から上記第2の端末装置へパケットが送出されたときに、上記パケットの受信側アドレスに対応するネットワークアクセス識別子を上記第2のルータ装置から受信し、その受信したネットワークアクセス識別子に対応するサービス情報を上記サービス情報保持手段から抽出して有効化する有効化手段と、有効化されたサービス情報に従ってサービスを提供する提供手段と、

10

20

30

40

50

4

を有することを特徴とするルータ装置。

【請求項10】 第1の端末装置を収容する第1のルータ装置、第2の端末装置を収容する第2のルータ装置、および上記第1および第2の端末装置に提供すべきサービスを規定するサービス情報を管理するサーバ装置を備えるサービス制御ネットワークにおいて、上記第1のルータ装置として使用されるルータ装置であって、上記第1の端末装置に提供すべきサービスを規定するサービス情報を上記サーバ装置から受信して保持するサービス情報保持手段と、上記第1の端末装置から上記第2の端末装置へパケットが送出されたときに、上記サービス情報保持手段から上記サービス情報を抽出し、上記第2のルータ装置に使用させるためにその抽出したサービス情報を上記第2のルータ装置へ送出する送出手段と、を有することを特徴とするルータ装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、加入者ごとに或いは端末ごとに個別のサービスを提供するサービス制御ネットワーク、サービス情報を配布する方法、サービスを提供する方法、および上記サービス制御ネットワークにおいて使用されるルータ装置に係わる。

【0002】

【従来の技術】 近年、インターネットの普及に伴い、膨大な数の端末装置がネットワークに接続できるようになっている。特に、ネットワークに接続可能な移動端末の数は急激に増加してきている。そして、このことに伴い、ネットワーク上に設けられる通信装置（主に、ルータ装置）の数も増加してきている。

【0003】 一方、加入者に通信サービスを提供するサービス提供業者は、各加入者との契約により、加入者ごとに異なったサービスを提供するようになってきている。例えば、端末ごとにQoS (Quality of Service)などを設定できるようになっている。

【0004】 ところで、各加入者または端末に対して個別のサービスを提供するためには、モバイル環境を考慮すると、ネットワーク上のすべての通信ノードに各加入者ごとのサービス制御情報を設定しておくことが望ましい。しかし、ネットワーク上に設けられている通信ノードの数は膨大であり、その全てに各加入者のサービス制御情報を設定しておくことは実質的に不可能である。

【0005】 このため、ネットワーク上の全ての通信ノードに各加入者のサービス制御情報を設定することなく、必要最小限の通信ノード（例えば、実際に設定される通信経路上の通信ノード）のみに対応する加入者のサービス制御情報を動的に設定する方式が提案されている。この方式は、例えば、移動端末がある通信ノードの通信エリアから他の通信ノードに通信エリアに移動した際に、その移動端末を新たに収容することとなった通信

ノードにその移動端末のサービス制御情報を配布することにより実現される。

【0006】

【発明が解決しようとする課題】ところで、現在、インターネット上で送受信されるパケットは、主に、IP v 4により定められているアドレス体系のアドレスを利用してルーティングされている。しかし、IP v 4はアドレス数が十分でなく、将来的には、次世代のアドレス体系であるIP v 6が使用されるようになると考えられている。

【0007】ところが、IP v 6ネットワークは、次世代のネットワークであり、現時点において未だ具体的に規定されていないプロトコルも多い。そして、IP v 6ネットワークにおいて必要最小限の通信ノードに対応する加入者のサービス制御情報を配布する手順も具体化されていないもののひとつである。

【0008】また、必要最小限の通信ノードに対応する加入者のサービス制御情報を設定する方式では、各サービス制御情報は、対応する端末装置のIPアドレスを検索キーとして管理されている。しかし、この方式では、ある端末装置に係わるサービス制御情報がその端末装置を収容する通信ノードに設定されている場合であっても、その端末装置またはその端末装置と通信している相手端末のIPアドレスが何らかの理由により変更されると、サービス制御情報を格納するデータベースからその通信ノードにサービス制御情報を再配布する必要があった。

【0009】本発明の課題は、加入者ごとまたは端末装置ごとに規定されるサービスを提供する手順を示すことである。また、本発明の他の課題は、加入者ごとまたは端末装置ごとに規定されるサービスを効率的に提供することである。

【0010】

【課題を解決するための手段】本発明のサービス制御ネットワークは、端末装置を収容するルータ装置および上記端末装置を認証するサーバ装置を備えて上記端末装置に対してサービスを提供する構成であって、上記ルータ装置が、上記端末装置からアドレス要求を受信したときに上記サーバ装置に対して認証要求を送出する要求手段と、上記サーバ装置から上記認証要求に対応する認証応答および上記端末装置のサービス情報を受信してそのサービス情報に従ってサービスを提供する提供手段と、上記端末装置に対して上記アドレス要求に対応するアドレス応答を送出する応答手段とを有し、上記サーバ装置が、上記認証要求に基づいて上記端末装置を認証し、上記認証要求に対応する認証応答および上記端末装置のサービス情報を上記ルータ装置へ送出する送出手段を有する。

【0011】上記発明によれば、端末を認証するためのプロトコルを利用してサービス情報を配布するネットワ

ークにおいて、アドレス割当てプロトコルと上記認証プロトコルとが連携しているので、端末に対するアドレス割当て手順の中でその端末に対応するルータ装置にサービス情報を配布できる。

【0012】なお、上記アドレス要求がICMP v 6によるアドレス要求であり、上記認証要求がAAAプロトコルであるとすると、IP v 6におけるアドレス割当てプロトコルであるICMP v 6と端末を認証するためのAAAプロトコルとが連携するので、IP v 6端末に対するアドレス割当て手順の中でそのIP v 6端末に対応するルータ装置にサービス情報を配布できる。

【0013】本発明の他の態様のサービス制御ネットワークは、第1の端末装置を収容する第1のルータ装置、第2の端末装置を収容する第2のルータ装置、および上記第1および第2の端末装置に提供すべきサービスを規定するサービス情報を管理するサーバ装置を備えて上記第1および第2の端末装置にサービスを提供する構成であって、上記第1のルータ装置に設けられて上記第1の端末装置に提供すべきサービスを規定するサービス情報を上記サーバ装置から受信して保持する第1のサービス情報保持手段と、上記第1のルータ装置に設けられて上記第1の端末装置に設定されているネットワークアクセス識別子と上記第1の端末装置に動的に割り当てられるアドレスとの対応関係を表すアドレス情報を保持する第1のアドレス情報保持手段と、上記第2のルータ装置に設けられて上記第2の端末装置に提供すべきサービスを規定するサービス情報を上記サーバ装置から受信して保持する第2のサービス情報保持手段と、上記第2のルータ装置に設けられて上記第2の端末装置に設定されているネットワークアクセス識別子と上記第2の端末装置に動的に割り当てられるアドレスとの対応関係を表すアドレス情報を保持する第2のアドレス情報保持手段と、上記第1の端末装置と上記第2の端末装置との間の通信を開始した後に上記第1のルータ装置と上記第2のルータ装置との間で対応するアドレス情報あるいはアドレス情報とサービス情報を転送する転送手段と、上記第1のサービス情報保持手段に保持されているサービス情報、上記第2のサービス情報保持手段に保持されているサービス情報、上記第1のアドレス情報保持手段に保持されているアドレス情報、上記第2のアドレス情報保持手段に保持されているアドレス情報、および上記転送手段により転送された情報の少なくとも一部を利用してサービスを提供する提供手段とを有する。

【0014】上記発明によれば、第1の端末装置と第2の端末装置との間の通信を開始された後に、第1のルータ装置と第2のルータ装置との間で対応するサービス情報および/またはアドレス情報が授受される。したがって、各端末装置が任意の位置に移動した場合であっても、予め指定されたサービスを確実に提供できる。

【0015】なお、上記サービス制御ネットワークにお

いて、各サービスを規定するサービス情報がそれぞれ対応する端末装置のネットワークアクセス識別子を利用して管理される構成とし、第1の端末装置から第2の端末装置へパケットが送出されたときに、第1および第2のアドレス情報保持手段のうちの少なくとも一方により保持されているアドレス情報をを利用して、上記パケットの送信側アドレスおよび受信側アドレスに対応するネットワークアクセス識別子を検出し、その検出されたネットワークアクセス識別子に対応するサービス情報を利用してサービスが提供されるようにしてよい。

【0016】この構成によれば、第2の端末装置のアドレスが変わったとしても、第1のルータ装置は、第2のルータ装置から対応するアドレス情報を受け取ることができるので、第2の端末装置のネットワークアクセス識別子を検出できる。よって、第1のルータ装置は、そのネットワークアクセス識別子を利用してサービス情報にアクセスすることにより、対応するサービスを提供できる。

【0017】また、上記サービス制御ネットワークにおいて、第1のルータ装置が、受信したパケットの送信側アドレスおよび受信側アドレスのライフタイムを個別に管理するアドレスキャッシュと、上記アドレスキャッシュにより管理されているアドレスのライフタイムが消滅したときに対応するアドレス情報をおよびサービス情報を削除または無効化する手段を有するようにしてよい。この構成によれば、一定期間以上使用されていないアドレスに対応するサービス情報が削除または無効化されるので、ルータ装置のメモリ領域を有効に利用できる。

【0018】本発明のルータ装置は、第1の端末装置を収容する第1のルータ装置、第2の端末装置を収容する第2のルータ装置、および上記第1および第2の端末装置に提供すべきサービスを規定するサービス情報を管理するサーバ装置を備えるサービス制御ネットワークにおいて、上記第1のルータ装置として使用されることを前提とし、上記第1の端末装置に提供すべきサービスを規定するサービス情報をおよび上記第2の端末装置に提供すべきサービスを規定するサービス情報をそれぞれ上記第1の端末装置および上記第2の端末装置に設定されているネットワークアクセス識別子と関連づけて保持するサービス情報保持手段と、上記第1の端末装置から上記第2の端末装置へパケットが送出されたときに上記パケットの受信側アドレスに対応するネットワークアクセス識別子を上記第2のルータ装置から受信してその受信したネットワークアクセス識別子に対応するサービス情報を上記サービス情報保持手段から抽出して有効化する有効化手段と、有効化されたサービス情報を従ってサービスを提供する提供手段とを有する。

【0019】上記発明によれば、第1の端末装置から第2の端末装置へのパケット送信が開始されると、当該ルータ装置は、第2のルータ装置から第2の端末装置のネ

ットワークアクセス識別子を取得する。したがって、当該ルータ装置は、第2の端末装置が任意の位置に移動した場合であっても、その第2の端末装置のネットワークアクセス識別子を利用してサービス情報にアクセスすることにより、対応するサービスを確実に提供できる。

【0020】本発明の他の態様のルータ装置は、第1の端末装置を収容する第1のルータ装置、第2の端末装置を収容する第2のルータ装置、および上記第1および第2の端末装置に提供すべきサービスを規定するサービス情報を管理するサーバ装置を備えるサービス制御ネットワークにおいて、上記第1のルータ装置として使用されることを前提とし、上記第1の端末装置に提供すべきサービスを規定するサービス情報を上記サーバ装置から受信して保持するサービス情報保持手段と、上記第1の端末装置から上記第2の端末装置へパケットが送出されたときに上記サービス情報保持手段から上記サービス情報を抽出して上記第2のルータ装置に使用させるためにその抽出したサービス情報を上記第2のルータ装置へ送出する送出手段とを有する。

【0021】上記発明によれば、第1の端末装置から第2の端末装置へのパケット送信が開始されると、当該ルータ装置は、第2のルータ装置に対して第1の端末装置のサービス情報を送出する。そして、第2の端末装置は、このサービス情報をを利用して対応するサービスを提供する。すなわち、当該ルータ装置は、第2のルータ装置に所定のサービスを実行させることができる。

【0022】

【発明の実施の形態】以下、本発明の実施形態について図面を参照しながら説明する。図1～図4は、本発明の実施形態のサービス制御ネットワークの構成を示す図である。なお、実施形態のサービス制御ネットワークは、IPv6ネットワークを含むことを前提とする。また、実施形態のサービス制御ネットワークは、端末装置を認証するAAA(Authentication, Authorization, and Accounting)サーバ、IPv6ネットワークを構成する通信ノードとしてのルータ装置、IPv6ネットワークと端末装置とを接続するアクセス網、および端末装置としてのIPv6ホストを含む。

【0023】図1に示すネットワークは、単一のドメインから構成されている。このドメインは、あるサービスプロバイダにより管理されている。また、このドメインに属するIPv6ホストは、AAAサーバ1により認証される。さらに、IPv6ホスト11、12は、それぞれIPv6プロトコルに従って通信を行う機能を備えた端末装置であり、それぞれこのドメインに属している。なお、IPv6ホスト11、12のユーザは、このドメインを管理するサービスプロバイダとの間で加入者契約をしている。そして、IPv6ホスト11、12は、それぞれ、エッジノード21、22に収容されている。なお、エッジノードは、例えば、IPv6ルータ装置によ

り実現される。

【0024】図2に示すネットワークは、複数のドメインから構成されている。そして、IPv6ホスト11および12のホームドメインにAAAサーバ1が設けられており、外部ドメインにはAAAサーバ2が設けられている。また、IPv6ホスト11は、ホームドメインの通信エリアから外部ドメインの通信エリアに移動しており、エッジノード22に収容されている。なお、IPv6ホスト11および12は、AAAサーバ1により認証される。すなわち、AAAサーバ1は、IPv6ホスト11および12に対してAAAHとして機能し、AAAサーバ2は、IPv6ホスト11および12に対してAAAL又はAAAFとして機能する。

【0025】図3に示すネットワークは、図2に示したネットワークと同様に、複数のドメインから構成されている。ただし、図2に示したネットワークは、各ドメインがそれぞれQoS等のサービスを提供する構成であるのに対し、図3に示すネットワークは、サービスを提供するドメインとサービスを提供出来ないドメインが接続された構成である。ここでは、ホームドメインではサービスが提供されるが、外部ドメインではサービスが提供されないものとする。なお、ホームドメインおよび外部ドメインは、ゲートウェイエッジノード31、コアネットワーク、ゲートウェイエッジノード32を介して互いに接続されている。

【0026】図4に示すネットワークは、モバイルIPv6をサポートしている。即ち、移動ノード(MN: Mobile Node)41は、モバイルIPv6に従ってIPv6ネットワークに接続する。そして、モバイルIPv6では、移動ノード41の位置がホームエージェント(HA: Home Agent)43に登録される。なお、移動ノード41の通信相手のことを、通信ノード(CN: Correspondent Node)42と呼ぶことにする。また、このネットワークでは、階層化モバイルIPv6が使用されているものとする。したがって、ホームドメインおよび外部ドメインには、それぞれモビリティアンカーポイント(MAP: Mobility Anchor Point)44、45が設けられている。

【0027】なお、図1～図4に示したAAAサーバ、エッジノード(en)、ゲートウェイエッジノード(GEN)、ホームエージェント(HA)、モビリティアンカーポイント(MAP)の構成および動作については、後で詳しく説明する。

【0028】次に、図5～図7を参照しながら、本実施形態のサービス制御ネットワークにおいて、サービス制御情報を配布する際の基本シーケンス、および配布されたサービス制御情報を使用する際の基本シーケンスを説明する。

【0029】図5は、サービス制御情報を配布する際の基本シーケンスを示す図である。ここでは、図2に示し

たネットワークをベースに説明する。また、ここでは、IPv6ホスト11のサービス制御情報をエッジノード22に配布する場合を示す。なお、IPv6ホスト11は、AAAサーバ(AAAH)1により認証されるものとする。また、IPv6ホスト11のサービス制御情報は、AAAサーバ1がアクセス可能なデータベース(SPDB)51に格納されているものとする。

【0030】IPv6ホスト11は、図5には示していないが、ネットワークから定期的にICMP広告を受信する。ここで、ICMP広告は、例えばルータ装置から各端末に送出されるメッセージであり、ここでは、エッジノード22からIPv6ホスト11にICMP広告が送られたものとする。

【0031】IPv6ホスト11は、ICMP広告を受信すると、必要に応じてエッジノード22に対してアドレス割当要求(ICMP-AA要求)を送出する。このアドレス割当要求は、新たなIPv6アドレスの割当てを要求するためのメッセージであり、ICMPv6において規定されている。なお、IPv6ホスト11は、例えば、IPアドレスを保持していない場合、先に割り当てられていたIPアドレスが消滅した場合、あるルータ装置の通信エリアから他のルータ装置の通信エリアに移動した場合などにアドレス割当要求を出力する。

【0032】エッジノード22は、アドレス割当要求を受信すると、IPv6ホスト11に割り当てるべきIPアドレスを決定すると共に、アドレス認証要求をAAAサーバ(AAAL)2に送り出し、AAAサーバ2はそのアドレス認証要求をAAAサーバ(AAAH)1に転送する。

【0033】AAAサーバ(AAAH)1は、上記アドレス認証要求を受信すると、IPv6ホスト11を認証すると共に、データベース(SPDB)51からIPv6ホスト11のサービス制御情報としてのサービスプロファイル(SP)を抽出する。そして、AAAサーバ(AAAH)1は、アドレス認証応答と共にIPv6ホスト11のサービスプロファイルを、AAAサーバ(AAAL)2を介してエッジノード22に送出する。

【0034】エッジノード22は、アドレス認証応答およびIPv6ホスト11のサービスプロファイルを受信すると、まず、そのサービスプロファイルを自装置内のキャッシュに格納する。そして、アドレス割当要求に対する応答として、アドレス割当応答(ICMP-AA要求)をIPv6ホスト11に返送する。

【0035】上記手順により、IPv6ホスト11に新たなIPv6アドレスが割り当てられる。そして、このアドレス割当手順と連携して、IPv6ホスト11がAAAサーバ(AAAH)1により認証されると共に、IPv6ホスト11のサービスプロファイルがそのIPv6ホスト11を収容しているエッジノード22に配布される。このように、本実施形態のネットワークでは、ICMPv6とAAAプロトコルが互いに連携している。

11

【0036】図6は、配布されたサービスプロファイルの管理方法を示す図である。なお、IPv6ホスト11のサービスプロファイルをエッジノード22に配布する手順は、図5に示した通りである。

【0037】エッジノード22において、配布されたサービスプロファイルは、対応する端末装置のネットワークアクセス識別子NAI (Network Access Identifier) をキーとして管理される。ここで、ネットワークアクセス識別子は、各端末に対して一意に割り当てられている識別情報であり、端末装置が移動した場合であっても変わることはない。なお、IPv6ホスト11のネットワークアクセス識別子は、アドレス割当要求 (ICMP-AAA要求) によりエッジノード22に通知される。

【0038】また、エッジノード22は、対応するサービスプロファイルが配布された端末装置のネットワークアクセス識別子と、その端末装置に割り当てられたIPv6アドレスとの対応関係を記述したホストアドレス情報 (HA) を保持する。なお、ネットワークアクセス識別子は、AAAサーバ1から送られてきたサービスプロファイルに含まれている。図6に示す例では、IPv6ホスト11のサービスプロファイルがエッジノード22に配布されると、IPv6ホスト11のネットワークアクセス識別子とIPv6ホスト11に新たに割り当てたIPv6アドレスとの対応関係を記述したホストアドレス情報 (HA) が生成されている。

【0039】図7は、エッジノードが通信相手のホストアドレス情報を取得するシーケンスを示す図である。ここでは、IPv6ホスト11がエッジノード22に収容されており、IPv6ホスト12がエッジノード21に収容されている。また、エッジノード22は、IPv6ホスト11のサービスプロファイルおよびホストアドレス情報を保持しており、エッジノード21は、IPv6ホスト12のサービスプロファイルおよびホストアドレス情報を保持している。そして、IPv6ホスト11からIPv6ホスト12へデータパケットが送出されたものとする。

【0040】エッジノード22は、上記通信が開始されたことを検出すると、IPv6ホスト12を収容するエッジノード21に対してNAI-SPC要求を送る。一方、エッジノード21は、この要求を受信すると、NAI-SPC応答を利用してIPv6ホスト12のホストアドレス情報 (HA2) をエッジノード22に送る。これにより、エッジノード22は、IPv6ホスト12のホストアドレス情報を取得する。すなわち、エッジノード22は、受信側ホストのネットワークアクセス識別子を取得する。ここで、エッジノード22は、送信側ホストのネットワークアクセス識別子を予め取得している。従って、エッジノードは、送信側ホストおよび受信側ホストのネットワークアクセス識別子を所有していることに

10

20

30

40

50

12

なる。そして、エッジノード22は、これらのネットワークアクセス識別子を利用してサービスプロファイルにアクセスすれば、送信側ホストがIPv6ホスト11であり且つ受信側ホストがIPv6ホスト12である通信に対して規定されているサービス情報を抽出することができる。これにより、対応するサービスが提供される。

【0041】次に、図8～図10を参照しながら、本実施形態のサービス制御ネットワークの動作の一例を示す。ここでは、IPv6ホスト11からIPv6ホスト12へデータを送信する場合を想定する。なお、IPv6ホスト11およびIPv6ホスト12は、図8に示すように、それぞれエッジノード22およびエッジノード21に収容されている。また、IPv6ホスト11のネットワークアクセス識別子は「aaa」であり、IPv6ホスト11には「IPアドレス=2001:0:1:2::2」が割り当てられている。一方、IPv6ホスト12のネットワークアクセス識別子は「bbb」であり、IPv6ホスト12には「IPアドレス=2001:0:1:1::1」が割り当てられている。

【0042】エッジノード22は、AAAサーバ (AAA-H) 1から配布されたIPv6ホスト11のサービスプロファイルを保持している。尚、サービスプロファイルを配布する手順は、図5を参照しながら説明した通りである。ここで、IPv6ホスト11のサービスプロファイルは、IPv6ホスト11のネットワーク識別子 (aaa) をキーとして管理されている。また、エッジノード22は、IPv6ホスト11に係わるホストアドレス情報を保持している。ここでは、IPv6ホスト11のIPv6アドレスとそのネットワークアクセス識別子との対応関係、およびIPv6ホスト11の通信相手であるIPv6ホスト12のIPv6アドレスとそのネットワークアクセス識別子との対応関係が保持されている。

【0043】上記ネットワークにおいて、IPv6ホスト11からIPv6ホスト12へデータパケットが送出されると、エッジノード22は、そのパケットの送信元IPアドレス (2001:0:1:2::2) および着信先IPアドレス (2001:0:1:1::1) を検出する。続いて、その1組のアドレスに対応する1組のネットワークアクセス識別子 (aaa及びbbb) をホストアドレス情報を参照して検出する。更に、サービスプロファイルキャッシュから、上記1組のネットワークアクセス識別子に対応するサービス情報を抽出する。そして、抽出したサービス情報を従ってIPv6ホスト11からIPv6ホスト12へ向かうパケットの転送を制御する。

【0044】続いて、図9に示すように、IPv6ホスト12が、エッジノード21の通信エリアからエッジノード23の通信エリアに移動したものとする。この場合、図5を参照しながら説明した手順により、IPv6ホスト12に新たなIPアドレス (2001:0:1:3::1) が割り当てられると共に、IPv6ホスト12が認

証される。また、この手順と連携して、IP v6 ホスト 12 のサービスプロファイルが対応する AAA サーバ 1 からエッジノード 23 に配布され、また、IP v6 ホスト 12 のネットワークアクセス識別子と新たな IP v6 アドレスとの対応関係を記述したホストアドレス情報 HA が作成される。

【0045】上記ネットワーク構成において、IP v6 ホスト 11 から IP v6 ホスト 12 へデータパケットが送出されるものとする。この時、このパケットの着信先 IP アドレスは、IP v6 ホスト 12 に新たに割り当てられている IP v6 アドレス (2001:0:1:3::1) である。一方、エッジノード 22 に保持されているホストアドレス情報 HA には、IP v6 ホスト 12 に割り当てられていた古い IP v6 アドレス (2001:0:1:1::1) が設定されている。このため、エッジノード 22 は、IP v6 ホスト 11 から受信したパケットに対応するサービスプロファイルを使用することができない。

【0046】そこで、エッジノード 22 は、図 7 に示した手順を実行することにより、IP v6 ホスト 12 を収容するエッジノード 23 から、IP v6 ホスト 12 のホストアドレス情報を取得する。このとき、エッジノード 23 は、NAT-SPC 要求に従って、IP v6 ホスト 12 のホストアドレス情報（場合によっては、IP v6 ホスト 12 のホストアドレス情報およびサービスプロファイル）をエッジノード 22 へ送出する。そして、エッジノード 22 は、図 10 に示すように、自装置内のホストアドレス情報 HA を更新する。この結果、エッジノード 22 は、IP v6 ホスト 11 から IP v6 ホスト 12 へ向かうパケットに対応するサービスプロファイルを利用できるようになり、そのパケットは、そのサービスプロファイルに従って制御されるようになる。

【0047】このように、本実施形態のサービス制御ネットワークでは、各エッジノードにおいて、IP v6 ホストのサービスプロファイルが対応するネットワークアクセス識別子により管理されると共に、IP v6 ホストのネットワークアクセス識別子と IP v6 アドレスとの対応関係が管理される。そして、端末装置間の通信の開始に起因して、対応するサービスを提供するために必要な情報がエッジノード間で送受信されるようになっている。このため、IP v6 ホストの IP アドレスが変更された場合であっても、AAA サーバからエッジノードにサービスプロファイルを再配布する必要がない。

【0048】もし、各エッジノードにおいて、IP v6 ホストのサービスプロファイルが対応する IP アドレスにより管理されるとすると、IP v6 ホストの IP アドレスが変更されるごとに、AAA サーバから対応するエッジノードにサービスプロファイルを再配布しなければならない。そして、そのような構成は、AAA サーバに過大な負荷を欠けることになる。

【0049】次に、本実施形態のサービス制御ネットワ

ークにおいて使用される各種メッセージのデータ構成を説明する。ここで、各種メッセージは、基本的には、IP v6 パケットに格納されて伝送される。尚、IP v6 パケットは、IP v6 ヘッダおよびペイロードから構成され、IP v6 ヘッダは、図 6 4 に示すように、「バージョン情報」「トラフィッククラス」「フローラベル」「ペイロード長」「次ヘッダ」「ホップリミット」「送信元アドレス (Source Address)」「受信先アドレス (Destination Address)」から構成される。

【0050】図 6 5 (a) は、ICMP-AA 要求メッセージの構成を示す図である。このメッセージは、ICMP 広告を受信した IP v6 ホストからルータ装置（エッジノード）へ送出されるメッセージであり、「AAA プロトコルメッセージ」「チャレンジオプション」「タイムスタンプオプション」「クライアント識別オプション」「セキュリティデータオプション」から構成される。そして、AAA プロトコルメッセージの構成は、図 6 5 (b) に示す通りである。また、AAA プロトコルメッセージには、図 6 5 (c) に示す AAA プロトコルメッセージオプションが付加されることがある。

【0051】図 6 6 (a) は、ICMP-AA 応答メッセージの構成を示す図である。このメッセージは、ICMP-AA 要求メッセージに対応してルータ装置（エッジノード）から IP v6 ホストへ返送されるメッセージであり、「AAA プロトコルメッセージ」「タイムスタンプオプション」「鍵応答オプション」から構成される。そして、AAA プロトコルメッセージの構成は、図 6 6 (b) に示す通りである。また、AAA プロトコルメッセージには、図 6 6 (c) に示す AAA プロトコルメッセージオプションが付加されることがある。

【0052】図 6 7 は、DIAMETER メッセージを伝送するパケットの構成を示す図である。DIAMETER メッセージは、図 6 7 (a) に示すように、SCTP パケットに格納され、その SCTP パケットが IP v6 パケットのペイロードに格納される。なお、DIAMETER は、AAA プロトコルのひとつである。

【0053】SCTP パケットは、図 6 7 (b) に示すように、SCTP 共通ヘッダおよび複数の「chunk」から構成される。尚、SCTP 共通ヘッダの構成は、図 6 7 (c) に示す通りである。ここで、着信先ポート番号として「DIAMETER」が指定されている。

【0054】DIAMETER メッセージは、図 6 7 (d) に示す DIAMETER ヘッダを有する。そして、このヘッダ内のコマンドコードにより、メッセージの種別が識別される。また、図 6 7 (e) に示すように、上記ヘッダに続く AVP 領域にメッセージに対応するデータが格納される。

【0055】図 6 8 (a) は、AHR (AMR) メッセージのデータ構成を示す図である。AHR メッセージは、既存の DIAMETER メッセージのひとつであり、ル

ータ装置（エッジノード）からAAAサーバへIPv6ホストの認証を要求するためのメッセージである。そして、このメッセージには、認証すべきIPv6ホストのネットワークアクセス識別子が設定されている。また、このメッセージは、本実施形態では、ICMP-AAA要求を含んでいる。

【0056】図68(b)は、AHA(AMA)メッセージのデータ構成を示す図である。AHRメッセージは、既存のDIA METERメッセージのひとつであり、AHRメッセージが生成されたときにAAAサーバからルータ装置（エッジノード）へ返送される。なお、このメッセージは、本実施形態では、ICMP-AAA応答を含んでいる。また、このメッセージは、本実施形態では、AAAサーバにより認証されたIPv6ホストのサービスプロファイルを格納できるようになっている。この場合、このサービスプロファイルは、「Profile Cache AVP」に格納される。

【0057】図69(a)は、ASRメッセージのデータ構成を示す図である。ASRメッセージは、この実施形態のネットワークにおいて新たに導入されたメッセージであり、階層化モバイルIPv6ネットワークにおいてモビリティアンカーポイントからAAAサーバに対して対応する移動ノードのサービスプロファイルを要求するメッセージである。なお、このメッセージのコマンドコードは、他のメッセージと異なる一意の値が使用される。

【0058】図69(b)は、ASAメッセージのデータ構成を示す図である。ASAメッセージは、この実施形態のネットワークにおいて新たに導入されたメッセージであり、階層化モバイルIPv6ネットワークにおいてAAAサーバからモビリティアンカーポイントへ返送されるメッセージである。なお、このメッセージは、ASRメッセージにより要求されたサービスプロファイルを格納するための領域を有している。また、このメッセージのコマンドコードは、他のメッセージと異なる一意の値が使用される。

【0059】図70(a)は、HHRメッセージのデータ構成を示す図である。HHRメッセージは、既存のDIA METERメッセージのひとつであり、AAAサーバからゲートウェイエッジノード、モバイルIPv6のホームエージェント、または階層化モバイルIPv6のモビリティアンカーポイントに対応する端末装置の位置を通知するためのメッセージである。尚、このメッセージは、本実施形態では、対応する端末装置または移動ノードのサービスプロファイルを格納できるようになっている。

【0060】図70(b)は、HHAメッセージのデータ構成を示す図である。HHAメッセージは、既存のDIA METERメッセージの1つであり、HHRメッセージを受信したゲートウェイエッジノード、モバイルIPv6

のホームエージェント、または階層化モバイルIPv6のモビリティアンカーポイントからAAAサーバに返送される。

【0061】図70(c)は、STRメッセージのデータ構成を示す図である。STRメッセージは、既存のDIAMETERメッセージのひとつであり、セッションの終了を要求するためのメッセージである。また、図70(d)は、STAメッセージのデータ構成を示す図である。STAメッセージは、既存のDIAMETERメッセージのひとつであり、STRメッセージに対応するメッセージである。

【0062】図71は、NAI-SPC要求メッセージのデータ構成を説明する図である。NAI-SPC要求メッセージは、この実施形態のネットワークにおいて新たに導入されたメッセージであり、図71(a)に示すように、UDPパケットの中に格納される。なお、UDPパケットは、IPv6パケットのペイロードに格納される。

【0063】NAI-SPC要求メッセージは、ルータ装置（エッジノード）間でNAI解決を要求するために使用される。この場合、このメッセージには、対応するネットワークアクセス識別子を見つけるIPv6アドレスが設定される。また、このメッセージは、ルータ装置（エッジノード）間でサービスプロファイルおよび/またはホストアドレス情報を送出するために使用することができる。

【0064】図71(b)は、UDPヘッダの構成を示す図である。また、図71(c)および図71(d)は、NAI-SPC要求に含まれるNAI-SPCプロトコルメッセージおよびNAI-SPCプロトコルメッセージオプションのデータ構成を示す図である。

【0065】図72は、NAI-SPC応答メッセージのデータ構成を説明する図である。NAI-SPC応答メッセージは、この実施形態のネットワークにおいて新たに導入されたメッセージであり、図72(a)に示すように、UDPパケットの中に格納される。

【0066】NAI-SPC応答メッセージは、NAI-SPC要求メッセージに対応するメッセージであり、サービスプロファイルおよび/またはホストアドレス情報を格納することができる。また、このメッセージは、要求されたNAI解決の結果を返送するために使用される。NAI-SPC応答に含まれるNAI-SPCプロトコルメッセージおよびNAI-SPCプロトコルメッセージオプションのデータ構成を図72(b)および図72(c)に示す。

【0067】図73は、結合更新メッセージのデータ構成を説明する図である。結合更新メッセージは、既存のDIAMETERメッセージのひとつであり、移動ノードの移動に際しての結合更新処理のための使用される。なお、このメッセージは、図73(a)に示すように、I

Pv6パケットのペイロードに格納される。結合更新メッセージのデータ構成を図73(b)に示す。

【0068】図74は、ICMP-AA-Teardown要求メッセージのデータ構成を説明する図である。この要求メッセージは、提供されているサービスの無効化を要求するメッセージであり、図74(a)に示すように「AAAプロトコルメッセージ」「チャレンジオプション」「タイムスタンプオプション」「クライアント識別オプション」「セキュリティデータオプション」から構成される。

【0069】図74(b)は、ICMP-AA-Teardown要求メッセージのAAAプロトコルメッセージのデータ構成である。また、図74(c)は、ICMP-AA-Teardown要求メッセージのAAAプロトコルメッセージオプションのデータ構成である。

【0070】図75は、ICMP-AA-Teardown応答メッセージのデータ構成を説明する図である。この応答メッセージは、ICMP-AA-Teardown要求メッセージに対応するメッセージであり、図75(a)に示すように、「AAAプロトコルメッセージ」「タイムスタンプオプション」から構成される。

【0071】図75(b)は、ICMP-AA-Teardown応答メッセージのAAAプロトコルメッセージのデータ構成である。また、図75(c)は、ICMP-AA-Teardown応答メッセージのAAAプロトコルメッセージオプションのデータ構成である。

【0072】次に、実施形態のサービス制御ネットワークを構成する機能エンティティ（AAAサーバ、ホームエージェントHA、モビリティアンカーポイントMA、エッジノードEN、ゲートウェイエッジノードGE、CN）について説明する。尚、IPv6ホストは、IPv6による通信を行うことができる加入者端末である。また、移動ノードMNは、モバイルIPv6による通信を行うことができる加入者端末である。ここで、これらの加入者端末は、イーサネット（登録商標）等の有線LAN、無線LAN、CDMA等の無線アクセス網に接続するための機能を備えている。通信ノードCNは、移動ノードと通信を行うIPv6ホストである。

#### AAAサーバの構成および動作

AAAサーバは、IPv6ホスト又は移動ノードの認証(Authentication)、認可(Authorization)、および課金(Accounting)を行う1または複数のサーバコンピュータであり、IETFにおいて使用されている名称である。AAAサーバに係わるプロトコルとしては、DIAMETER<draft-calhoun-diameter-12.txt>、<draft-calhoun-diameter-mobileip-07.txt>が知られている。なお、ある加入者から見て、その加入者について認証/認可、課金を実行するAAAサーバこのとを「AAAH(AAA Home)」と呼ぶ。一方、ある加入者から見てAAA以外のAAAサーバを「AAAF(AAA Fore

ign)」または「AAAL(AAA Local)」と呼ぶ。

【0073】本実施形態のサービス制御ネットワークにおいて使用されるAAAサーバは、上記基本機能に加え、加入者端末にIPv6アドレスが割り当てられる際に、その加入者端末のNAI（ネットワークアクセス識別子）に対応するサービス制御情報としてのサービスプロファイルをデータベース(SPDB)51から抽出し、そのサービスプロファイルを上記加入者端末を収容するルータ装置等に配布するための機能を備える。

【0074】図11は、AAAサーバの機能ブロック図である。ネットワークインターフェース101は、IPv6ネットワークに接続する回線を終端する。

【0075】プロトコル制御部102は、ネットワークインターフェース101を介して受信したパケットを解析し、そのパケットの種別に応じて対応する処理を実行する。そして、受信パケットが本実施形態に係わるメッセージを含んでいた場合は、プロトコル制御部102は、そのメッセージに対応する処理をサービスデータ管理部103に要求する。例えば、サービスプロファイルデータベース104から対応するサービスプロファイルを抽出する要求や、サービス規定データ105へのアクセス要求などが作成される。

【0076】サービスデータ管理部103は、プロトコル制御部102からの要求に応じてサービスプロファイルデータベース104またはサービス規定データ105にアクセスする。

【0077】サービスプロファイルデータベース104は、当該AAAサーバが管理するドメインに属する各加入者のサービス制御情報（サービスプロファイル）を格納する。サービスプロファイルデータベース104に格納されるサービスプロファイルの一例を図12に示す。サービスプロファイルデータベース104は、基本的に、サービスごとにサービスプロファイルが登録されており、各サービスプロファイルは、そのサービスを受ける加入者のNAIをキーとして管理される。サービス情報としては、QoSクラス等が設定される。

【0078】サービスプロファイルは、1:1のIPv6ホスト間の通信だけでなく、1:多のIPv6ホスト間通信、多:1のIPv6ホスト間通信、多:多のIPv6ホスト間通信を記述することもできる。サービスプロファイルにおいて複数のIPv6ホストを設定する場合は、ワイルドカードを利用してIPv6アドレスを指定してもよいし、ネットマスクを適切に設定してもよい。例えば、図8～図10に示すネットワークにおいて、IPv6ホスト11から外部ドメイン2に収容されるすべての端末装置へ送信されるパケットのQoSを一括して記述する場合は、「送信側IPv6アドレス」と「受信側IPv6アドレス」としてそれぞれ「2001:0:1:2::2」と「2001:0:1:3::\*」を設定しておけばよい。

【0079】サービス規定データ105は、当該AAAサーバがAAAALとして動作する場合に、AAAHから配布されたサービスプロファイルおよびホストアドレス情報を格納する。なお、サービスプロファイルはオリジナルサービスプロファイルキャッシュ(OSPC)に格納され、ホストアドレス情報はオリジナルホストアドレスキャッシュ(OHAC)に格納される。

【0080】図13(a)は、オリジナルサービスプロファイルキャッシュ(OSPC)の実施例である。オリジナルサービスプロファイルキャッシュ(OSPC)は、IPV6ホスト毎に、かつサービス毎にサービスプロファイルを格納する。ここで、各サービスプロファイルは、管理すべきIPV6ホストのNAI(NAI-ID)をキーとして登録される。登録される情報は、「送信側NAI」「送信側IPV6アドレス」「送信側ネットマスク」「送信側ポート番号」「受信側NAI」「受信側IPV6アドレス」「受信側ネットマスク」「受信側ポート番号」「サービス情報」などである。ただし、必ずしもこれらの全てが登録されている必要はない。

【0081】例えば、図8に示すネットワークにおいて、IPV6ホスト11のサービスプロファイルを格納するオリジナルサービスプロファイルキャッシュ(OSPC)は、以下のようなになる。ただし、IPV6ホスト11からIPV6ホスト12へのデータ送信に係わるサービスを規定するものとする。

【0082】管理ホストNAI識別子：aaa

送信側NAI：aaa

送信側IPV6アドレス：

送信側ネットマスク：

送信側ポート番号：

受信側NAI：bbb

受信側IPV6アドレス：

受信側ネットマスク：

受信側ポート番号：

サービス情報：QoS=高優先度

図13(b)は、オリジナルホストアドレスキャッシュ(OHAC)の例である。オリジナルホストアドレスキャッシュ(OHAC)には、管理すべきIPV6ホストのNAI(NAI-ID)をキーとして、「管理ホストアドレスIPV6アドレス」「有効時間」「AAA関連情報」「送出先IPV6アドレス」などが登録される。なお、「管理ホストアドレスIPV6アドレス」は、管理すべきIPV6ホストに割り当てられているIPV6アドレスである。したがって、IPV6ホストに割り当てられるIPV6アドレスが変更されると、それに伴って「管理ホストアドレスIPV6アドレス」が更新される。これにより、常に、IPV6ホストのNAIと現在のIPV6アドレスとの対応関係が登録されることになる。「有効時間」は、当該IPV6アドレスに対応するサービスプロファイルが有効に使用できる残り時間である。「送出先

IPV6アドレス」は、当該エンティティから他のエンティティにサービスプロファイルを配布した場合に、その送り先のエンティティのIPV6アドレスを表す。

【0083】図14～図16は、AAAサーバのプロトコル制御部102の動作を示すフローチャートである。この処理は、ネットワークインターフェース101からメッセージを受信したときに実行される。

【0084】ステップS1では、アドレス認証要求を受信したか否かを調べる。ここで、アドレス認証要求は、DIAMETERプロトコルのAHRメッセージが利用される。なお、DIAMETERメッセージの種別は、例えば、図67(a)に示したDIAMETERヘッダのコマンドコードにより検出される。

【0085】アドレス認証要求を受信した場合は、ステップS2において、そのメッセージの宛先が当該AAAサーバであるか否かを調べる。そして、そのメッセージの宛先が当該AAAサーバであればステップS3以降の処理が実行され、そうでない場合は、ステップS9へ進む。

【0086】ステップS3～S8の処理は、AAAHによって実行される。ステップS3では、認証処理を実行すると共に、アドレス認証要求に設定されているIPV6ホストのNAIに対応するサービスプロファイルの抽出をサービスデータ管理部103に要求する。ステップS4では、サービスデータ管理部103から対応するサービスプロファイルを受け取る。

【0087】ステップS5では、アドレス認証要求に係わるIPV6ホストの位置(アドレス)を登録するためのホームエージェントが存在するか否かを調べる。なお、ホームエージェントは、モバイルIPV6ネットワークにおいて設けられる。ステップS6では、ゲートウェイエッジノードが存在するか否かを調べる。ゲートウェイエッジノードは、例えば、図3に示したネットワークに設けられる。

【0088】ホームエージェントおよびゲートウェイエッジノードの双方が存在しない場合は、ステップS7において、アドレス認証応答を作成する。なお、アドレス認証応答は、ステップS4で取得したサービスプロファイルを含んでおり、DIAMETERプロトコルのAH Aメッセージが利用される。一方、ホームエージェントまたはゲートウェイエッジノードが存在する場合は、ステップS8において、設定要求を作成する。なお、設定要求は、ステップS4で取得したサービスプロファイルを含んでおり、DIAMETERプロトコルのHHRメッセージが利用される。

【0089】ステップS9では、作成したメッセージを格納するパケットをネットワークインターフェース101に渡す。これにより、作成したメッセージがネットワークに送出される。

【0090】ステップS11では、削除要求を受信した

か否かを調べる。ここで、削除要求は、D I A M E T E RプロトコルではS T Rメッセージである。削除要求を受信した場合は、ステップS 1 2において、サービスデータ管理部1 0 3に削除要求を送る。この削除要求は、不図示のセッション情報を削除する要求を含む。そして、ステップS 1 3においてサービスデータ管理部1 0 3から削除応答を受信すると、ステップS 1 4において、削除応答を作成する。なお、この削除応答は、ステップS 9においてパケットに格納され、削除要求の送信元に返送される。

【0091】ステップS 2 1では、アドレス認証応答を受信したか否かを調べる。なお、アドレス認証応答は、D I A M E T E RプロトコルではA H Aメッセージである。そして、アドレス認証応答を受信した場合は、ステップS 2 2～S 2 5の処理が実行される。ここで、ステップS 2 2～S 2 5の処理は、A A A Lにより実行される。

【0092】ステップS 2 2では、サービスデータ管理部1 0 3に対して設定要求を送る。ここで、この設定要求は、アドレス認証要求と共に送られてきたサービスプロファイルをサービス規定データ1 0 5に格納する指示である。そして、ステップS 2 3において上記設定要求に対応する設定応答を受信すると、ステップS 2 4において、モビリティアンカーポイントが存在するか否かを調べる。なお、モビリティアンカーポイントは、後で詳しく説明するが、階層化モバイルI P v 6ネットワークにおいて存在する。

【0093】モビリティアンカーポイントが存在する場合は、ステップS 2 5において、設定要求を作成する。尚、この設定要求は、ステップS 8で作成した設定要求と同じであるが、宛先はモビリティアンカーポイントである。一方、モビリティアンカーポイントが存在しない場合は、ステップS 2 5をスキップする。この場合、受信したアドレス認証応答がそのまま回送される。

【0094】ステップS 3 1では、設定応答を受信したか否かを調べる。この設定応答は、設定要求に対応するメッセージであり、D I A M E T E RプロトコルではH A H Aメッセージである。そして、設定応答を受信した場合は、ステップS 3 2において、上記設定応答の送信元がゲートウェイエッジノードであるか否かが調べられる。

【0095】ゲートウェイエッジノードから設定応答を受信したのであれば、ステップS 3 3において、アドレス認証応答を作成する。この場合、アドレス認証応答は、サービスプロファイルを含んでいない。一方、ゲートウェイエッジノード以外のエンティティから設定応答を受信したのであれば、ステップS 3 4およびS 3 5において、対応するサービスプロファイルを取得する。この場合、ステップS 3 3で作成されるアドレス認証応答は、サービスプロファイルを含んでいる。

【0096】ステップS 4 1では、抽出要求を受信したか否かを調べる。なお、この抽出要求は、サービスプロファイルの配布を要求するメッセージであり、本実施形態では、図6 9 (a)に示したA S Rメッセージにより実現される。抽出要求を受信した場合には、ステップS 4 2において抽出要求をサービスデータ管理部1 0 3に送り、ステップS 4 3において対応するサービスプロファイルを取得する。そして、ステップS 4 4において抽出応答を作成する。この抽出応答は、本実施形態では、図6 9 (b)に示したA S Aメッセージにより実現される。また、この抽出応答は、ステップS 4 3で取得したサービスプロファイルを含んでいる。

【0097】なお、受信パケットが、アドレス認証要求、削除要求、アドレス認証応答、設定応答または抽出要求を格納していなかった場合は、ステップS 4 5において、他の処理を実行する。

【0098】このように、プロトコル制御部1 0 2は、受信メッセージに基づいて対応するメッセージを作成すると共に、必要に応じて、対応するサービスプロファイルの抽出／設定／削除に係わる要求をサービスデータ管理部1 0 3に送る。そして、サービスプロファイルを取得した場合は、作成したメッセージと共に対応するエンティティに送出する。

【0099】図1 7は、A A Aサーバのサービスデータ管理部1 0 3の動作を示すフローチャートである。この処理は、プロトコル制御部1 0 2から要求を受け取ったときに実行される。

【0100】ステップS 5 1～S 5 3では、抽出要求、設定要求、または削除要求を受信したか否かが調べられる。削除要求を受信した場合は、ステップS 5 4においてサービス規定データ1 0 5から対応する情報を削除した後、ステップS 5 5において削除応答をプロトコル制御部1 0 2へ送出する。なお、ステップS 5 4およびS 5 5の処理は、A A A Lにおいて実行される。

【0101】設定要求を受信した場合は、ステップS 5 6において、サービスプロファイルおよび／またはホストアドレス情報をサービス制御データ1 0 5に設定する。その後、ステップS 5 7において設定応答をプロトコル制御部1 0 2へ送出する。なお、ステップS 5 6およびS 5 7の処理は、A A A Lにおいて実行される。

【0102】抽出要求を受信した場合は、ステップS 5 8において、サービスプロファイルデータベース1 0 4またはサービス制御データ1 0 5から対応するサービスプロファイルを抽出する。なお、A A A Hは、サービスプロファイルデータベース1 0 4からサービスプロファイルを抽出し、A A A Lは、サービス制御データ1 0 5からそれを抽出する。そして、ステップS 5 9において抽出応答と共に抽出したサービスプロファイルをプロトコル制御部1 0 2へ送出する。

50 ホームエージェントおよびモビリティアンカーポイント

## の構成および動作

ホームエージェント (Home Agent) は、モバイルIP v 6 ネットワークにおいて移動ノードのホームアドレスを所有するエンティティであり、移動ノードの位置を登録するためのテーブルを備える。そして、移動ノードのホームアドレス宛てのパケットを受信すると、そのパケットをカプセル化してその移動ノードの気付アドレス (Care-of-Address) 宛てに転送する機能を有する。ここで、「移動ノードの気付けアドレス」とは、移動ノードが移動先のドメインにおいて割り当てられるIPアドレスである。

【0103】本実施形態のホームエージェントは、上記基本機能に加え、AAAサーバから配布された移動ノードのサービスプロファイルをキャッシュする機能、そのサービスプロファイルに係わるホストアドレス情報を生成してキャッシュする機能、キャッシュ済みサービスプロファイルおよびホストアドレス情報を抽出して転送する機能を有する。

【0104】モビリティアンカーポイント (Mobility Anchor Point) は、ホームエージェント機能を階層化した階層化モバイルIP v 6において、外部ドメインにおいて下位のホームエージェントとして動作するエンティティである。モビリティアンカーポイントの役割について図18を参照しながら説明する。

【0105】階層化モバイルIP v 6では、移動ノード (MN) の位置は、RCOA (Regional Care-of-Address) およびLCOA (Local Care-of-Address) により識別される。RCOAは、移動ノードが位置する通信エリアを管理するモビリティアンカーポイント (MAP) を識別するアドレスであり、LCOAは、各モビリティアンカーポイントが管理するエリア内で使用されるアドレスである。

【0106】図18において、移動ノード (MN) があるモビリティアンカーポイント (MAP-A) が管理するエリアから他のモビリティアンカーポイント (MAP-B) が管理するエリアにローミングインしたときは、ホームエージェントに対してRCOAが通知され、モビリティアンカーポイント (MAP-B) に対してLCOAが通知される。一方、移動ノードが、1つのモビリティアンカーポイントが管理するエリア内で移動したときは、そのモビリティアンカーポイントに位置登録を行なうが、ホームエージェントへの位置登録は行わない。これにより、ホームエージェントへのアクセスが減少するので、ネットワークの負荷が軽くなると共に、移動ノードの移動に伴う処理の高速化が実現される。なお、モビリティアンカーポイントについては、IETFが発行している<draft-ietf-mobileip-hmipv6-02.txt>に詳しく記載されている。

【0107】本実施形態のモビリティアンカーポイントは、上記基本機能に加え、AAAサーバあるいはエッジ

ノードから配布された移動ノードのサービスプロファイルをキャッシュする機能、そのサービスプロファイルに係わるホストアドレス情報を生成してキャッシュする機能、キャッシュ済みサービスプロファイルおよびホストアドレス情報を抽出して転送する機能を有する。

【0108】図19は、ホームエージェント、モビリティアンカーポイントの機能ブロック図である。ネットワークインターフェース201は、IP v 6 ネットワークに接続する回線を終端する。

【0109】プロトコル制御部202は、ネットワークインターフェース201を介して受信したパケットを解析し、そのパケットの種別に応じて対応する処理を実行する。そして、受信パケットが本実施形態に係わるメッセージを含んでいた場合は、プロトコル制御部202は、そのメッセージに対応する処理をサービスデータ管理部203に要求する。例えば、サービス規定データ204へのアクセス要求などが作成される。

【0110】サービスデータ管理部203は、プロトコル制御部202からの要求に応じてサービス規定データ204にアクセスする。サービス規定データ204は、基本的に、AAAサーバが備えるサービス規定データ105と同じである。

【0111】図20～図21は、ホームエージェントまたはモビリティアンカーポイントのプロトコル制御部202の動作を示すフローチャートである。この処理は、ネットワークインターフェース201からメッセージを受信したときに実行される。

【0112】ステップS61では、NAI-SPC要求を受信したか否かを調べる。NAI-SPC要求の構成は、図71に示した通りである。NAI-SPC要求を受信した場合は、ステップS62において、サービスデータ管理部203に対して対応するサービスプロファイルの抽出を要求する。そして、ステップS63において抽出応答と共にサービスプロファイルを受け取ると、ステップS64においてNAI-SPC応答を作成する。なお、このNAI-SPC応答は、ステップS63で受け取ったサービスプロファイルを含んでいる。

【0113】ステップS65では、作成したメッセージを格納するパケットをネットワークインターフェース201に渡す。これにより、作成したメッセージがネットワークに送出される。

【0114】ステップS71では、設定要求を受信したか否かが調べられる。この設定要求は、対応するサービスプロファイルを含んでおり、本実施形態では、DIAMETERプロトコルのHHRメッセージにより実現される。

【0115】設定要求を受信した場合は、ステップS72において、その設定要求に含まれているサービスプロファイルをサービス規定データ204に設定する旨をサービスデータ管理203に要求する。そして、ステップ

S 7 3において上記設定要求に対応する設定応答を受信すると、ステップS 7 4において、設定応答を作成する。この設定応答は、D I A M E T E Rプロトコルでは、H H Aメッセージである。

【0116】ステップS 8 1では、結合更新(Binding Update)を受信したか否かが調べられる。結合更新を受信した場合は、ステップS 8 2において、その結合更新がI Pv 6ホストのサービスプロファイルを含んでいるか否かを調べる。

【0117】結合更新がI Pv 6ホストのサービスプロファイルを含んでいる場合は、ステップS 8 3およびS 8 4が実行される。すなわち、設定要求に含まれているサービスプロファイルをサービス規定データ2 0 4に設定する旨をサービスデータ管理2 0 3に要求し、対応する設定応答を受信する。一方、結合更新がI Pv 6ホストのサービスプロファイルを含んでいなかった場合は、ステップS 8 5において、抽出要求を作成する。この抽出要求は、図6 9 (a)に示すA S Rメッセージにより実現される。

【0118】ステップS 8 6では、抽出応答を受信したか否かを調べる。ここで、この抽出応答は、図6 9 (b)に示すA S Aメッセージにより実現される。また、この抽出応答には、ステップS 8 5で作成した抽出応答に従って抽出されたサービスプロファイルが格納されている。そして、抽出応答を受信した場合は、ステップS 8 3およびS 8 4が実行される。

【0119】なお、受信パケットが、N A I - S P C要求、設定要求、結合更新または抽出応答を格納しなかった場合は、ステップS 8 7において他の処理を実行する。このように、プロトコル制御部2 0 2は、受信メッセージに基づいて対応するメッセージを作成すると共に、必要に応じて、対応するサービスプロファイルの抽出／設定に係わる要求をサービスデータ管理部1 0 3に送る。そして、サービスプロファイルを取得した場合は、作成したメッセージを共に対応するエンティティに送出する。

【0120】ホームエージェントまたはモビリティアンカーポイントのサービスデータ管理部2 0 3の動作は、基本的に、図1 7に示したA A Aサーバのサービスデータ管理部1 0 3の動作と同じである。したがって、ここではその説明を省略する。

エッジノードおよびゲートウェイエッジノードの構成および動作

エッジノード(Edge Node)は、ドメインのエッジに位置するI Pv 6ルータ装置である。本実施形態のエッジノードは、一般的なルーティング機能の他、以下の4つの機能を有する。

【0121】(1) 加入者端末にI Pv アドレスを割り当てる時に、A A Aサーバから配布されたサービス情報(サービスプロファイル)、およびそのサービス情報をもと

に生成するホストアドレス情報をキャッシュする機能。

【0122】(2) 加入者端末の通信開始時に、通信相手端末のホストアドレス情報および／またはサービス情報を取得する機能。

(3) 予め保有しているサービス情報を有効化することによりサービス制御を実行する機能。

【0123】(4) 加入者端末のデータ送信終了後に、サービス情報を無効化または削除することによりサービス制御を中止する機能。ゲートウェイエッジノード(Gateway Edge Node)は、各プロバイダネットワークのゲートウェイに位置するI Pv 6ルータ装置である。本実施形態のゲートウェイエッジノードは、一般的なゲートウェイ機能に加え、上記エッジノードの機能(1)～(4)を有する。

【0124】図2 2は、エッジノードおよびゲートウェイエッジノードの機能ブロック図である。ネットワークインターフェース3 0 1は、I Pv 6ネットワークに接続する回線を終端する。

【0125】サービス制御部3 0 2は、ネットワークインターフェース3 0 1を介してパケットを受け取ると、そのパケットの送信側ホストのI Pv 6アドレスおよび受信側ホストのI Pv 6アドレスがサービス制御データ3 0 8内のアドレスキャッシュ(ADC)にキャッシュされているか否かをチェックする。そして、双方のホストのI Pv 6アドレスがキャッシュされているれば、それらのホスト間の通信のためのサービス情報が有効状態であると判断し、パケット編集部3 0 3に対してサービスの実行を要求する。一方、送信側ホストまたは受信側ホストの少なくとも一方のI Pv 6アドレスがキャッシュされていなかった場合は、ネットワークインターフェース3 0 1を介して受信したパケットをプロトコル制御部3 0 4に送ると共に、サービスデータ管理部3 0 5に対してヒットミス通知を送出する。また、上記アドレスキャッシュ(ADC)を定期的に監視し、各I Pv 6アドレス毎に設定されているライフタイムの満了を検出した際に、サービスデータ管理部3 0 5に対してライフタイムオーバーを通知する。なお、アドレスチェック処理、およびライフタイムカウント処理は、アドレスキャッシュ(ADC)の構成により異なる。

【0126】パケット編集部3 0 3は、サービス制御部3 0 2を介してパケットを受信すると、そのパケットの送信側ホスト及び受信側ホストに対応するサービス情報(サービスプロファイル)をサービス制御データ3 0 8内のポリシテーブル(PT)から抽出し、そのサービス情報に従ってサービスを提供する。そして、必要に応じて、そのパケットをネットワークインターフェース3 0 1を介してネットワークに送出する。

【0127】プロトコル制御部3 0 4は、サービス制御部3 0 2を介して受信したパケットを解析し、そのパケットの種別に対応する処理を実行する。具体的には、受

信パケットが本実施形態に係わるメッセージを含んでいれば、サービスデータ管理部305に対して、サービス規定データ306へのアクセス（各種情報の抽出、設定、削除）、サービス実行データ307およびサービス制御データ308へのアクセス（各種情報の設定、削除）を要求する。

【0128】サービスデータ管理部305は、プロトコル制御部304からの要求に応じてサービス規定データ306へのアクセス（各種情報の抽出、設定、削除）、サービス実行データ307およびサービス制御データ308へのアクセス（各種情報の設定、削除）を実行する。また、サービス制御部302からのヒットミス通知を受信したときは、パケットの受信側ホストのホストアドレス情報および／またはサービス情報を取得するために、プロトコル制御部304に対して、N A I - S P C 要求メッセージの生成を要求する。一方、ライフタイムオーバー通知を受信したときは、サービス実行データ307およびサービス制御データ308内の対応する情報を無効化または削除する。なお、サービス実行データ307およびサービス制御データ308の設定処理および削除処理は、アドレスキャッシュ（ADC）の構成により異なる。

【0129】サービス規定データ306は、当該ノードに収容されるIPv6ホストに対するアドレス割当てに際してAAAサーバから配布されたサービス情報を格納するオリジナルサービスプロファイルキャッシュ（OSPC）、及びそのIPv6ホストのホストアドレス情報を格納するオリジナルホストアドレスキャッシュ（CHAC）から構成される。なお、サービス規定データ306は、基本的に、AAAサーバが備えるサービス規定データ105と同じである。

【0130】サービス実行データ307は、当該ノードに収容されるIPv6ホストが他のIPv6ホストと通信している場合、それらのホストのサービス情報（サービスプロファイル）を格納するコミュニケーションサービスプロファイルキャッシュ（CSPC）、およびそれらのホストのホストアドレス情報を格納するコミュニケーションホストアドレスキャッシュ（CHAC）から構成される。

【0131】図23(a)及び図23(b)は、それぞれコミュニケーションサービスプロファイルキャッシュ（CSPC）内の送信側サービスプロファイルキャッシュ（SSPC）および受信側サービスプロファイルキャッシュ（DSPC）の例である。「サービスプロファイル識別子」は、IPv6ホスト毎かつサービス毎に作成されているサービスプロファイルを識別する識別子である。「送信側N A I」～「サービス情報」は、基本的に、サービス規定データ306に格納されている情報がそのまま設定される。「サービス実行状態」は、コミュニケーションサービスプロファイルキャッシュ（CSPC）内に設定

されている「送信側N A I」～「サービス情報」が使用可能な状態であるか否かを表示する。

【0132】図23(c)および図23(d)は、それぞれコミュニケーションホストアドレスキャッシュ（CHAC）内の送信側ホストアドレスキャッシュ（SHAC）および受信側ホストアドレスキャッシュ（DHAC）の例である。これらのキャッシュには、送信側IPv6ホストのN A IとIPv6アドレスとの対応関係、および受信側IPv6ホストのN A IとIPv6アドレスとの対応関係が格納される。

【0133】図24は、サービス実行データ307の作成方法を説明する図である。ここでは、エッジノードAに収容されているIPv6ホストAからエッジノードBに収容されているIPv6ホストBへパケットが転送される場合を想定する。また、ここでは、エッジノードAのサービス実行データ307を設定する場合を説明する。

【0134】送信側サービスプロファイルキャッシュ（SSPC）には、送信側ホストであるIPv6ホストAのサービスプロファイルが設定される。ここで、IPv6ホストAのサービスプロファイルは、IPv6ホストAを収容するエッジノードAのサービス規定データ306に格納されている。したがって、送信側サービスプロファイルキャッシュ（SSPC）に設定すべきサービスプロファイルは、エッジノードAのサービス規定データ306から取得する。

【0135】一方、受信側サービスプロファイルキャッシュ（DSPC）には、受信側ホストであるIPv6ホストBのサービスプロファイルが設定される。ここで、IPv6ホストBのサービスプロファイルは、IPv6ホストBを収容するエッジノードBのサービス規定データ306に格納されている。したがって、受信側サービスプロファイルキャッシュ（DSPC）に設定すべきサービスプロファイルは、エッジノードBのサービス規定データ306から取得する。

【0136】同様に、送信側ホストアドレスキャッシュ（SHAC）に設定すべきホストアドレス情報は、エッジノードAのサービス規定データ306から取得し、受信側ホストアドレスキャッシュ（DHAC）に設定すべきホストアドレス情報は、エッジノードBのサービス規定データ306から取得する。

【0137】なお、図24に示す例では、送信側ホストを収容するエッジノードのサービス実行データを設定する例を示したが、受信側ホストを収容するエッジノードにおいても同様にサービス実行データを設定してもよい。

【0138】サービス制御データ308は、サービス実行データ307において有効化されているサービス情報（サービスプロファイル）をキャッシュするポリシーブル（PT）、およびサービス実行データ307において

有効化されているサービス情報に対応するIP v6ホストのIP v6アドレスをキャッシュするアドレスキャッシュ(ADC)から構成される。なお、アドレスキャッシュ(ADC)は、送信側アドレスおよび受信側アドレスを個別に管理する構成であってもよいし、各サービスに対応する送信側アドレスおよび受信側アドレスの組合せを管理する構成であってもよい。

【0139】図25(a)～図25(c)は、送信側ホストおよび受信側ホストのIP v6アドレスを個別に管理する場合の、送信側アドレスキャッシュ(SAC)、受信側アドレスキャッシュ(DAC)、及びポリシーテーブル(PT)の例である。この場合、送信側IP v6アドレスおよび受信側IP v6アドレスのそれぞれについてライフタイムが管理される。

【0140】図26(a)および図26(b)は、サービス毎に送信側ホスト及び受信側ホストのIP v6アドレスの組合せを管理する場合の、アドレスキャッシュ(ADC)、およびポリシーテーブル(PT)の例である。この場合、ポリシーテーブル(PT)は、1組の送信側IP v6ホストおよび受信側IP v6ホストを識別するためのサービスプロファイル識別子をキーとして管理される。

【0141】なお、送信側アドレスおよび受信側アドレスを個別に管理する構成は、アドレスキャッシュ(ADC)を作成するためのメモリサイズが小さくなる。一方、サービス毎に送信側アドレスおよび受信側アドレスの組合せを管理する構成は、アドレスキャッシュ(ADC)の検索時間が短くなる。

【0142】ところが、上述したように、エッジノードのサービス実行データ307には、1セットの通信における送信側ホストのサービスプロファイルおよび受信側ホストのサービスプロファイルが設定されることがある。たとえば、図24に示した例では、エッジノードAのサービス実行データ307内に、IP v6ホストAからIP v6ホストBへのパケット転送に係わるサービスについてIP v6ホストAに対して規定されているサービスプロファイル、および同じサービスについてIP v6ホストBに対して規定されているサービスプロファイルが格納されている。すなわち、サービス実行データ307内には、ある1つのサービスに対して2セットのサービスプロファイルが設定されていることになる。

【0143】このため、エッジノードは、1つのサービスに対して1セットのサービスプロファイルが使用されるようにするために、優先度の高いサービスプロファイルを有効化し、他のサービスプロファイルを無効化する。そして、サービス実行データ307において有効化されたサービスプロファイルが、サービス制御データ308内のポリシーテーブル(PT)に登録される。

【0144】図27は、エッジノードまたはゲートウェイエッジノードのサービス制御部302の動作を示すフローチャートである。この処理は、所定間隔ごとに実行

される。

【0145】ステップS91では、ネットワークインターフェース301を介してパケットを受信しているか否かを調べる。ステップS92では、受信パケットの宛先が当該エッジノードに収容されているIP v6ホストであるか否かを調べる。そして、受信パケットの宛先が当該エッジノードに収容されているIP v6ホストであれば、ステップS98において、そのパケットをプロトコル制御部304に送出する。

【0146】受信パケットの宛先が当該エッジノードに収容されているIP v6ホストでなかった場合は、ステップS93およびS94において、そのパケットの送信元アドレスおよび着信先アドレスがサービス制御データ308のアドレスキャッシュ(ADC)に格納されているか否かをチェックする。そして、アドレスキャッシュ(ADC)にヒットした場合は、ステップS95において、サービス制御データ308のポリシーテーブル(PT)に従ってパケットを編集する。ここで、「編集」とは、例えば、パケットのヘッダを書き換える処理等を含む。一方、アドレスキャッシュ(ADC)にヒットしなかった場合は、ステップS96において、そのパケットをプロトコル制御部304に渡す。また、ステップS97において、ヒットミス通知をサービスデータ管理部305へ送る。

【0147】パケットを受信しない場合(ステップS91:No)は、ステップS99及びS100において、サービス制御データ308のアドレスキャッシュ(ADC)により管理されているライフタイム(有効時間)をチェックする。そして、受信パケットの送信元アドレスまたは着信先アドレスのライフタイムが終了していた場合は、ステップS101において、ライフタイムオーバ通知をサービスデータ管理部305へ送る。一方、ライフタイムが残存している場合は、ステップS101はスキップされる。なお、サービス制御データ308のアドレスキャッシュ(ADC)により管理されている各IP v6アドレスのライフタイムは、周期的にデクリメントされている。

【0148】図28および図29は、アドレスキャッシュをチェックする処理のフローチャートであり、図27のステップS93に相当する。ここで、図28は、送信側アドレスおよび受信側アドレスを個別に管理する場合のフローチャートであり、図25(a)及び図25(b)に示したアドレスキャッシュがチェックされる。一方、図29は、各サービスに対応する送信側アドレスおよび受信側アドレスの組合せを管理する場合のフローチャートであり、図26(a)に示したアドレスキャッシュがチェックされる。

【0149】図28において、ステップS111およびS112では、受信パケットのヘッダに設定されている送信元アドレスが、サービス制御データ308のアドレ

スキヤッッシュ (ADC) 内の送信側アドレスキャッシュ (SAC) に格納されているか否か調べる。そして、送信側アドレスキャッシュ (SAC) にヒットしなかった場合は、ステップS113において、ヒットミス通知メッセージを作成すると共に、そのメッセージに対応するミス要因を書き込む。なお、送信側アドレスキャッシュ (SAC) にヒットした場合は、ステップS113はスキップされる。

【0150】同様に、ステップS114およびS115では、受信パケットのヘッダに設定されている着信先アドレスが受信側アドレスキャッシュ (DAC) に格納されているか否かを調べる。そして、受信側アドレスキャッシュ (DAC) にヒットしなかった場合は、ステップS116において、ヒットミス通知メッセージに対応するミス要因を書き込む。

【0151】図29において、ステップS121及びS122では、受信パケットのヘッダに設定されている1組の送信元アドレスおよび着信先アドレスが、サービス制御データ308のアドレスキャッシュ (ADC) に格納されているか否かを調べる。そして、アドレスキャッシュ (ADC) にヒットしなかった場合は、ステップS123において、ヒットミス通知メッセージを作成し、そのメッセージに対応するミス要因を書き込む。なお、アドレスキャッシュ (ADC) にヒットした場合は、ステップS123はスキップされる。

【0152】このように、送信側アドレスまたは受信側アドレスの少なくとも一方についてヒットミスが発生すると、その旨を通知するためのヒットミス通知メッセージが作成される。

【0153】図30は、エッジノードまたはゲートウェイエッジノードのパケット編集部303の動作を示すフローチャートである。この処理は、サービス制御部302から編集要求を受け取ったときに実行される。なお、サービス制御部302は、受信パケットの送信元アドレスおよび着信先アドレスがサービス制御データ308のアドレスキャッシュに格納されていたときに編集要求を出力する。

【0154】ステップS131では、受信パケットに対応する情報 (サービスプロファイル等) をサービス制御データ308のポリシーテーブル (PT) から抽出する。ステップS132では、ポリシーテーブル抽出した情報に基づいてパケットを編集する。そして、ステップS133において、ネットワークインターフェース301を介して編集したパケットを送出する。

【0155】図31～図34は、エッジノードまたはゲートウェイエッジノードのプロトコル制御部304の動作を示すフローチャートである。この処理は、サービス制御部302からパケットを受信したとき、またはサービスデータ管理部305からパケット生成要求を受信したときに実行される。

【0156】ステップS141では、サービス制御部302からパケットを受信したか否かを調べる。ステップS142では、受信パケットにNAI-SPC要求メッセージが含まれているか否かを調べる。そして、受信パケットにNAI-SPC要求メッセージが含まれていた場合は、ステップS143において、そのメッセージの中に抽出要求が含まれているか否かを調べる。

【0157】NAI-SPC要求メッセージの中に抽出要求が含まれていれば、ステップS144において、サービスデータ管理部305へ抽出要求を送る。ここで、抽出要求は、サービス規定データ306から対応するサービスプロファイルおよび／またはホストアドレス情報を抽出する要求である。ステップS145では、抽出応答として、サービス規定データ306から対応するサービスプロファイルおよび／またはホストアドレス情報を受け取る。ステップS146では、NAI-SPC応答メッセージを作成する。このメッセージは、ステップS145で取得したサービスプロファイルおよび／またはホストアドレス情報が格納されている。そして、ステップS150において、作成したメッセージを格納するパケットを送出する。

【0158】NAI-SPC要求メッセージの中に抽出要求が含まれていれば、ステップS147において、サービスデータ管理部305へ設定要求又は削除要求を送る。ここで、設定要求は、NAI-SPC要求メッセージと共に送られてきたサービスプロファイルおよび／またはホストアドレス情報をサービス実行データ307に設定する要求である。一方、削除要求は、NAI-SPC要求メッセージにおいて指定されているサービスプロファイルおよび／またはホストアドレス情報をサービス実行データ307から削除する要求である。そして、ステップS148においてサービスデータ管理305から設定応答または削除応答を受け取ると、ステップS149において、NAI-SPC応答メッセージを作成する。

【0159】ステップS151では、受信パケットにICMP-AAA要求メッセージが含まれているか否かが調べられる。そして、受信パケットにICMP-AAA要求メッセージが含まれていれば、ステップS152において、ICMP-AAA要求を出したIPv6ホストに割り当てるべきIPv6アドレスを決定すると共に、そのアドレスに対応するアドレス認証要求を作成する。そして、ステップS153において、上記アドレス認証要求を含むAHRメッセージを作成する。

【0160】ステップS154では、受信パケットにアドレス認証応答メッセージが含まれているか否かが調べられる。そして、受信パケットにアドレス認証応答メッセージが含まれていれば、ステップS155において、そのアドレス認証応答メッセージと共に送られてきたサービスプロファイルをサービス規定データ306に設定

する旨の要求をサービスデータ管理部305に送る。また、ステップS156では、上記ICMP-AAA要求を送出したIPv6ホストについてのホストアドレス情報を作成する。なお、このホストアドレス情報は、サービス規定データ306のオリジナルホストアドレスキャッシュ(OHAC)に設定される。そして、ステップS157において、上記ICMP-AAA要求を送出したIPv6ホストへ送出すべきICMP-AAA応答メッセージを作成する。

【0161】ステップS161では、受信パケットに結合更新メッセージが含まれているか否かを調べる。そして、受信パケットに結合更新メッセージが含まれている場合は、ステップS162において対応するIPv6ホストのサービスプロファイルをモビリティアンカーポイント(MAP)に設定する必要があるか否か調べる。

【0162】モビリティアンカーポイント(MAP)に対応するサービスプロファイルを設定する場合は、ステップS163およびS164においてサービスプロファイルを取得する。なお、ステップS163およびS164の処理は、ステップS144およびS145と同じである。そして、ステップS165において、取得したサービスプロファイルを含む結合更新メッセージを作成する。

【0163】ステップS171では、受信パケットに削除応答メッセージが含まれているか否か調べる。ここで、削除応答メッセージは、STAメッセージにより実現される。ステップS172では、サービスデータ管理部305に対して、削除応答メッセージに対応するサービスプロファイルおよび/またはホストアドレス情報の削除を要求する。

【0164】ステップS173においてサービスデータ管理部305から削除応答を受信すると、ステップS174において、他のエッジノードに削除すべきサービスプロファイルおよび/またはホストアドレス情報が存在するか否かを調べる。なお、ステップS172～S173において削除したサービスプロファイルおよび/またはホストアドレス情報を先に他のエッジノードに送出していた場合には、それらを削除する必要がある。そして、当該エッジノードから他のエッジノードへサービスプロファイルおよび/またはホストアドレス情報を送出した場合は、その送り先のアドレスがサービス規定データ306の「送出先IPv6アドレス」として記録されている(図13(b)参照)。

【0165】他のエッジノードに削除すべきサービスプロファイルおよび/またはホストアドレス情報が存在する場合は、ステップS175において、NAI-SPC要求メッセージを作成する。一方、そのような情報が存在しない場合は、ステップS176において、AAA-Teardown応答メッセージを作成する。

【0166】ステップS181では、受信パケットにN

AI-SPC応答メッセージが含まれているか否かを調べる。ステップS182では、受信したNAI-SPC応答メッセージの中に削除応答が含まれているか否かを調べる。そして、削除応答が含まれていれば、ステップS183において、AAA-Teardown応答メッセージを作成する。一方、削除応答が含まれていなければ、ステップS184およびS185において、サービスデータ管理部305へ設定要求を送出する。この設定要求は、NAI-SPC応答メッセージと共に送られてきたサービスプロファイルおよび/またはホストアドレス情報をサービス実行データ307に設定すべき旨を要求する。

【0167】ステップS191では、受信パケットに設定要求メッセージが含まれているか否かを調べる。ステップS192では、サービスデータ管理部305に対して設定要求が送られる。そして、ステップS193においてサービスデータ管理部305から設定応答を受信すると、ステップS194において、設定応答メッセージを作成する。

【0168】ステップS201では、受信パケットにAAA-Teardown要求メッセージが含まれているか否かを調べる。そして、AAA-Teardown要求メッセージが含まれていた場合は、ステップS202において削除要求メッセージを作成する。ここで、削除要求メッセージは、STRメッセージにより実現される。

【0169】なお、受信したパケットが、NAI-SPC要求、ICMP-AAA要求、アドレス認証応答、結合更新、削除応答、NAI-SPC応答、設定要求、またはAAA-Teardown要求を含んでいなかった場合は、ステップS203において、他のパケット処理が実行される。

【0170】ステップS211では、サービスデータ管理部305からパケット生成要求を受け取ったか否か調べる。そして、パケット生成要求を受け取っている場合は、ステップS212において、対応するパケット(ここでは、NAI-SPC要求を含むパケット)を生成する。

【0171】図35は、エッジノードまたはゲートウェイエッジノードのサービスデータ管理部305の動作を示すフローチャートである。この処理は、プロトコル制御部304から要求を受信したとき、またはサービス制御部302から通知を受信したときに実行される。

【0172】ステップS221～S225では、プロトコル制御部304から受信した要求またはサービス制御部302から受信した通知の種別を検出する。抽出要求を受信した場合は、ステップS226において、指定されたサービスプロファイルおよび/またはホストアドレス情報をサービス規定データ306から抽出する。そして、ステップS227において、抽出した情報をプロトコル制御部304へ送る。

【0173】設定要求を受信した場合は、ステップS2

28において、その要求と共に送られてきたサービスプロファイルおよび／またはホストアドレス情報をサービス規定データ306またはサービス実行データ307へ設定する。そして、必要に応じて設定応答をプロトコル制御部304に返送する。

【0174】削除要求を受信した場合は、ステップS229において、指定されたサービスプロファイルおよび／またはホストアドレス情報をサービス規定データ306またはサービス実行データ307から削除する。そして、必要に応じて削除応答をプロトコル制御部304に返送する。  
10

【0175】ヒットミス通知を受信した場合は、ステップS230において対応するヒットミス処理を実行する。また、ライフタイムオーバ通知を受信した場合は、ステップS231において対応するライフタイムオーバ処理を実行する。

【0176】図36および図37は、アドレスキャッシュにおいてヒットミスが発生した場合の処理のフローチャートであり、図35のステップS230に相当する。ここで、図36は、送信側アドレスおよび受信側アドレスを個別に管理する場合のフローチャートであり、図37は、各サービスに対応する送信側アドレスおよび受信側アドレスの組合せを管理する場合のフローチャートである。

【0177】図36において、ステップS241では、送信側IPv6アドレスについてキャッシュミス(送信側ヒットミス)が発生したか否かを調べる。キャッシュミスの種別は、サービス制御部302により作成されるヒットミス通知に設定されている。送信側ヒットミスが発生した場合は、ステップS242において、受信パケットの送信元アドレスに対応する情報をサービス規定データ306から抽出する。具体的には、オリジナルサービスプロファイルキャッシュ(OSPC)から対応するサービスプロファイルを抽出すると共に、オリジナルホストアドレスキャッシュ(OHAC)から対応するホストアドレス情報を抽出する。

【0178】ステップS243では、ステップS242で抽出した情報をサービス規定データ307に設定する。具体的には、サービスプロファイルが送信側サービスプロファイルキャッシュ(SSPC)に設定され、ホストアドレス情報が送信側ホストアドレスキャッシュ(SHA-C)に設定される。このとき、送信側サービスプロファイルキャッシュ(SSPC)に設定されるサービスプロファイルは、有効化される。すなわち、図23(a)において、「サービス実行状態=有効」が設定される。そして、ステップS244において、ステップS243で有効化されたサービスプロファイルがサービス制御データ308のポリシーブル(PT)に設定され、対応するIPv6アドレスがサービス制御データ308のアドレスキャッシュ内の送信側アドレスキャッシュ(SAC)に設  
50

定される。

【0179】ステップS245では、受信側IPv6アドレスについてキャッシュミス(受信側ヒットミス)が発生したか否かを調べる。受信側ヒットミスが発生した場合は、ステップS246において、NAI-SPC要求メッセージを含むパケットを生成するためのパケット生成要求を作成する。ここで、このパケット生成要求は、プロトコル制御部304に送られる。また、NAI-SPC要求メッセージは、受信パケットに設定されている着信先アドレスに対応するサービスプロファイルおよび／またはホストアドレス情報を、着信先ホストを収容するエッジノードから取得するためのメッセージである。

【0180】各サービスが対応する送信側アドレスおよび受信側アドレスの組合せにより管理されている場合は、図37に示すように、ヒットミスが発生したときに上述のパケット生成要求がプロトコル制御部304に送られる。

【0181】なお、図36のステップS242～S244の処理は、ヒットミスが発生したパケットに設定されている着信先アドレスについてのサービスプロファイルだけでなく、他のサービスプロファイルに対して実行されることもある。例えば、図38に示すネットワークを想定する。ここでは、エッジノードXにIPv6ホストAおよびIPv6ホストCが収容されており、エッジノードYにIPv6ホストBおよびIPv6ホストDが収容されている。また、現在、IPv6ホストCからIPv6ホストDへデータ送信中であるものとする。この場合、エッジノードXのサービス制御データ308において、送信側アドレスキャッシュには「IPv6ホストC」が設定され、受信側アドレスキャッシュには「IPv6ホストD」が設定されている。

【0182】上記構成において、IPv6ホストAからIPv6ホストBへのデータ送信が開始されるものとする。ここで、IPv6ホストAのアドレスがエッジノードXの送信側アドレスキャッシュに格納されていないとすると、送信側ヒットミスが発生し、図36のステップS242～S244が実行される。この結果、エッジノードXの送信側アドレスキャッシュには「IPv6ホストA」および「IPv6ホストC」が設定され、受信側アドレスキャッシュには「IPv6ホストB」および「IPv6ホストD」が設定されることになる。

【0183】上記送信側ヒットミスの発生に際して、エッジノードXにおいては、IPv6ホストAからIPv6ホストBへのデータ送信に係わるサービスプロファイルが有効化される。このとき、受信側アドレスキャッシュには「IPv6ホストB」だけでなく「IPv6ホストD」も設定されている。このため、もし、IPv6ホストAからIPv6ホストDへのデータ送信が開始されると、エッジノードXでは、ヒットミスが生じないこと

になる。すなわち、この場合、IP v6ホストAからIP v6ホストDへのデータ送信に係わるサービスプロファイルがサービス制御データ308のポリシーテーブル(Pt)に設定されている必要がある。したがって、エッジノードXにおいては、上記送信側ヒットミスの発生に際して、IP v6ホストAから、受信側アドレスキャッシュに設定されている各着信先アドレスへの通信に係わるサービスプロファイルをそれぞれ有効化しておく必要がある。

【0184】また、図36のステップS242～S244は、サービス実行データ307において1つのサービスに対して2以上のサービスプロファイルが設定されている場合は、それらの中の1つを有効化するように実行される。例えば、図24に示した例では、エッジノードAのサービス実行データ307内に、IP v6ホストAからIP v6ホストBへのパケット転送に係わるサービスについて、IP v6ホストAに対して規定されているサービスプロファイルおよびIP v6ホストBに対して規定されているサービスプロファイルが格納されている。ここで、前者のサービスプロファイルはエッジノードAのサービス規定データ306から抽出したものであり、後者のサービスプロファイルはエッジノードBから取得したものである。そして、この場合、これら2つのサービスプロファイルの一方のみが有効化される。なお、1つのサービスに対して複数のサービスプロファイルが設定されている場合に、それら複数のサービスプロファイルの中から1つのサービスプロファイルを有効化する処理のことを「マージ」と呼ぶことにする。

【0185】図39は、サービスプロファイルをマージする処理のフローチャートである。ステップS261では、有効化すべきサービスプロファイル(対象サービスプロファイル)を初期化する。具体的には、サービス実行データ307内の対応する領域をクリアする。ステップS262では、対象サービスプロファイルが規定するサービスと同じサービスについて規定するサービスプロファイル(候補サービスプロファイル)が他に存在するか否かを調べる。そして、候補サービスプロファイルが存在する場合は、ステップS263において、対象サービスプロファイルおよび候補サービスプロファイルの中から1つのサービスプロファイルを選択する。ステップS264では、ステップS263で選択されたサービスプロファイルを有効化する。

【0186】図40は、図39の選択処理の実施例を記載したフローチャートである。すなわち、図39のステップS263は、ステップS271およびS272として記載されている。なお、この実施例では、各サービスプロファイルに対して予め優先度が設定されているものとする。

【0187】ステップS271では、対象サービスプロファイルの優先度と候補サービスプロファイルの優先度

とを比較する。そして、対象サービスプロファイルの優先度の方が高ければ、そのままステップS262に戻る。一方、候補サービスプロファイルの優先度の方が高ければ、その候補サービスプロファイルを対象サービスプロファイルとしてステップS262に戻る。そして、すべての候補サービスプロファイルについてステップS271およびS272の処理を実行することにより、最も優先度の高いサービスプロファイルが選択される。従って、ステップS264において、最も優先度の高いサービスプロファイルが有効化される。

【0188】図41および図42は、IP v6アドレスのライフタイムオーバが発生した場合の処理のフローチャートであり、図35のステップS231に相当する。ここで、図41は、送信側アドレスおよび受信側アドレスが個別に管理される場合のフローチャートであり、図42は、各サービスが対応する送信側アドレスおよび受信側アドレスの組合せにより管理される場合のフローチャートである。

【0189】図41において、ステップS281では、サービス制御データ308内の送信側アドレスキャッシュ(SAC)においてライフタイムオーバが発生したか否かを調べる。なお、ライフタイムオーバが送信側アドレスキャッシュで発生したのか受信側アドレスキャッシュで発生したのかは、サービス制御部302により作成されるライフタイムオーバ通知に設定されている。

【0190】送信側アドレスキャッシュにおいてライフタイムオーバが発生した場合は、ステップS282において、そのライフタイムオーバが発生したIP v6アドレスに対応する情報がサービス制御データ308内のポリシーテーブルおよび送信側アドレスキャッシュから削除される。ステップS283では、上記ライフタイムオーバが発生したIP v6アドレスに対応する情報がサービス実行データ307内の送信側サービスプロファイルキャッシュおよび送信側ホストアドレスキャッシュから削除される。そして、ステップS284において、サービス実行データ307の受信側サービスプロファイルキャッシュにおいて、上記ライフタイムオーバが発生したIP v6アドレスに対応するサービスプロファイルを無効化する。例えば、図38に示すネットワークにおいて、IP v6ホストAに割り当てられているIP v6アドレスのライフタイムが消滅したとすると、エッジノードXの受信側サービスプロファイルキャッシュにおいて、IP v6ホストBおよびIP v6ホストDについてのサービスプロファイルが無効化される。

【0191】受信側アドレスキャッシュにおいてライフタイムオーバが発生した場合の処理は、基本的には、送信側アドレスキャッシュにおいてライフタイムオーバが発生した場合と同じである。ただし、受信側アドレスキャッシュにおいてライフタイムオーバが発生した場合は、ステップS288において、受信側サービスプロ

アイルキャッシュ (DSCP) および受信側ホストアドレスキャッシュ (DHAC) から対応する情報が削除される。

【0192】各サービスが送信側アドレスおよび受信側アドレスの組合せにより管理されている場合は、任意の IPv6アドレスのライフタイムが消滅すると、図42に示すように、サービス制御データ308のアドレスキャッシュ (ADC) 及びポリシーブル (PT) において対応する情報が削除され、サービス実行データ307の送信側サービスプロファイルキャッシュ (SSPC) および送信側ホストアドレスキャッシュ (SHAC) において対応する情報が削除／無効化され、サービス実行データ307の受信側サービスプロファイルキャッシュ (DSCP) および送受信ホストアドレスキャッシュ (DHAC) において対応する情報が削除／無効化される。

#### 実施例

上記構成のサービス制御ネットワークにおける動作についての実施例を説明する。以下では、実施例1～7において、IPv6ホストのアドレス割当てあるいは結合更新時に、そのホストに対応するサービス情報を通信経路上のノードに配布するシーケンスを示す(図7、図8参照)。また、実施例8～12において、IPv6ホストの通信開始時に、サービス制御を実行するエッジノードが相手ホストのホストアドレス情報および／またはサービスプロファイルを取得するシーケンスを示す(図9参照)。さらに、実施例13～16では、エッジノードにおいて所定のサービス情報を有効化するシーケンスを示す。また、実施例17～21では、IPv6アドレスのライフタイムの消滅時またはIPv6ホストの通信終了時にサービス情報を無効化するシーケンスを示す。

【0193】なお、以下の実施例では、AAAプロトコルとしてDIAMETERプロトコルを利用しているが、本発明はこれに限定されるものではない。

#### 実施例1

実施例1は、図1に示したネットワーク構成を前提とする。そして、IPv6ホスト11がホームドメインにおいてアドレス割当てを要求する際に、AAAサーバ(AAAH)1がIPv6ホスト11を収容するエッジノード21にサービス情報を配布する。以下、図43を参照しながら、サービス情報の配布シーケンスを説明する。なお、本実施例および後続する実施例2～5のシーケンスは、IPv6ホスト11または移動ノード41がエッジノード21、22からICMP広告メッセージを受信したときに開始されるものとする。

【0194】(1) IPv6ホスト11は、IPv6ホスト11のNAIおよびAAA証明書を含むICMP-AIA要求メッセージをエッジノード21へ送信する。  
(2) ICMP-AIA要求メッセージを受信したエッジノード21は、エッジノード21が属するドメイン内に存在するAAAサーバに対して、上記NAIおよびAAA証明書を含むAHR(アドレス認証要求)メッセージ

を送信する。すなわち、AAAサーバ(AAAH)1にAHRメッセージが送られる。この処理は、図31のステップS152およびS153により実現される。

【0195】(3) AHRメッセージを受信したAAAサーバ(AAAH)1は、AAA証明書に基づいてIPv6ホスト11を認証する。また、受信したNAIを検索キーとしてサービスプロファイルデータベース(SPDB)104にアクセスし、対応するサービス情報(サービスプロファイル)を抽出する。この処理は、図14のステップS3、図17のステップS58により実現される。

【0196】(4) AAAサーバ(AAAH)1は、エッジノード21に対して、上記(3)で抽出したサービスプロファイルを含むAHA(アドレス認証応答)メッセージを送信する。この処理は、図14のステップS7、S9により実現される。

【0197】(5) AHAメッセージを受信したエッジノード21は、受信したサービスプロファイルに基づいて対応する情報をサービス規定データ306に設定する。具体的には、受信したサービスプロファイルをオリジナルサービスプロファイルキャッシュ(OSPC)に設定し、また、IPv6ホスト11のNAIとIPv6ホスト11に割り当てるべきIPv6アドレスとの対応関係を表示するホストアドレス情報をオリジナルホストアドレスキャッシュ(OHAC)に設定する。そして、IPv6ホスト11に対して、ICMP-AIA応答メッセージを送信する。この処理は、図31のステップS154～S156により実現される。

【0198】上記シーケンスにより、IPv6ホスト11を収容するエッジノード21は、IPv6ホスト11のサービス情報を取得する。すなわち、IPv6ホスト11がエッジノード21の通信エリア内で電源を投入したとき、あるいはIPv6ホスト11があるノードの通信エリアからエッジノード21の通信エリアに移動したときは、そのエッジノード21にIPv6ホスト11のサービス情報が設定されることになる。また、エッジノード21は、IPv6ホスト11のNAIと新たに割り当てられたIPv6アドレスとの対応関係を保持する。よって、エッジノード21は、IPv6ホスト11が送受信するパケットに対して対応するサービスを提供できる。

#### 実施例2

実施例2は、図2に示したネットワーク構成を前提とする。そして、IPv6ホスト11が外部ドメインにおいてアドレス割当てを要求する際に、AAAサーバ(AAAH)1がIPv6ホスト11を収容するエッジノード22にサービス情報を配布する。ここで、AAAサーバ(AAAH)1は、IPv6ホスト11のホームドメインに設けられている。以下、図44を参照しながら、サービス情報の配布シーケンスを説明する。

【0199】(1) 実施例1の(1)と同様に、IPv6ホ

41

スト11からエッジノード22へICMP-AA要求メッセージが送信される。

(2) 実施例1の(2)と同様に、エッジノード22からAAAサーバへAHRメッセージが送信される。ただし、このメッセージは、AAALであるAAAサーバ(AAAH)2に送られる。

【0200】(3) AHRメッセージを受信したAAAサーバ(AAAH)2は、受信したメッセージに格納されているNAIに基づいてIPv6ホスト11のホームドメインを認識し、AAAHであるAAAサーバ(AAAH)1に10に対して上記AHRメッセージを回送する。なお、この処理は、図14のステップS2で「No」と判断されることにより実現される。

【0201】(4) 実施例1の(3)と同様に、IPv6ホスト11のサービスプロファイルが抽出される。

(5) 実施例1の(4)と同様に、AAAサーバ(AAAH)1からAHAメッセージが送出される。ただし、このメッセージは、いったんAAAServer(AAAH)2に送られる。

【0202】(6) AAAサーバ(AAAH)2は、受信したAHAメッセージをエッジノード22に回送する。20

(7) 実施例1の(5)と同様に、エッジノード22からIPv6ホスト11へICMP-AA応答メッセージが送信される。

【0203】上記シーケンスによれば、IPv6ホスト11が外部ドメインに移動した場合であっても、そのIPv6ホスト11を収容するエッジノード22に対応するサービス情報が配布される。したがって、IPv6ホスト11は、外部ドメインに移動しても、ホームドメインに位置しているときと同様のサービスを受けることができる。30

### 実施例3

実施例3は、図3に示したネットワーク構成を前提とする。そして、IPv6ホスト11が外部ドメインにおいてアドレス割当てを要求する際に、AAAサーバ(AAAH)1がホームドメインに設けられているゲートウェイエッジノード31にサービス情報を配布する。ここで、AAAサーバ(AAAH)1は、IPv6ホスト11のホームドメインに設けられている。また、IPv6ホスト11のホームドメインは、IPv6ホスト11に対して予め契約されているサービスを提供できるが、エッジノード22が位置している外部ドメインは、そのようなサービスを提供できないものとする。以下、図4.5を参照しながら、サービス情報の配布シーケンスを説明する。

【0204】(1)～(3) 実施例2の(1)～(3)と同様に、IPv6ホスト11からICMP-AA要求メッセージが送出され、そのICMP-AA要求メッセージを受信したエッジノード22からAAAHであるAAAServer(AAAH)1へAHRメッセージが送信される。

【0205】(4) 実施例2の(4)と同様に、IPv6ホ

42

スト11のサービスプロファイルが抽出される。

(5) 上記AHRメッセージが外部ドメイン(サービス非適用ドメイン)から送出されているので、AAAサーバ(AAAH)1は、上記(4)で抽出したサービスプロファイルを含むHHR(設定要求)メッセージをホームドメイン内のゲートウェイエッジノード31へ送信する。この処理は、図14のステップS6、S8、S9により実現される。

【0206】(6) HHRメッセージを受信したゲートウェイエッジノード31は、そのメッセージに含まれているサービスプロファイルに対応する情報をサービス規定データ204に設定する。具体的には、受信したサービスプロファイルをオリジナルサービスプロファイルキャッシュ(OSPC)に設定し、また、IPv6ホスト11のNAIとIPv6ホスト11に割り当てるべきIPv6アドレスとの対応関係を表示するホストアドレス情報をオリジナルホストアドレスキャッシュ(CHAC)に設定する。そして、AAAサーバ(AAAH)1に対してHHA(設定応答)メッセージを返送する。この処理は、図20のステップS72～S74により実現される。

【0207】(7)～(9) 実施例2の(5)～(7)と同様に、AAAサーバ(AAAH)1からAAAServer(AAAH)2を介してエッジノード22へAHAメッセージが送信され、エッジノード22からIPv6ホスト11へICMP-AA応答メッセージが送信される。ただし、この実施例では、外部ドメインがサービス非適用ドメインであるので、AAAサーバ(AAAH)1からエッジノード22へサービスプロファイルは配布されない。

【0208】上記シーケンスによれば、IPv6ホスト11がサービス非適用ドメインに移動した場合であっても、ホームドメイン内に設けられているゲートウェイエッジノード31にIPv6ホスト11のサービス情報が配布される。したがって、例えば、図3に示すネットワークにおいてIPv6ホスト11とIPv6ホスト12との間で通信が行われる場合には、ゲートウェイエッジノード31とIPv6ホスト12との間の通信に対してIPv6ホスト11が契約しているサービスが提供される。

### 実施例4

実施例4は、図4に示したネットワーク構成を前提とする。そして、移動ノード41が外部ドメインにおいてアドレス割当てを要求する際、AAAサーバ(AAAH)1がホームエージェント42および移動ノード41を収容するエッジノード22にサービス情報を配布する。以下、図4.6を参照しながら、サービス情報の配布シーケンスを説明する。

【0209】(1)～(3) 実施例3の(1)～(3)と同様に、移動ノード41からICMP-AA要求メッセージが送出され、そのICMP-AA要求メッセージを受信したエッジノード22からAAAServer(AAAH)1

へAHRメッセージが送信される。

【0210】(4) 実施例3の(4)と同様に、IPv6ホスト11のサービスプロファイルが抽出される。

(5) モバイルIPv6環境においてAHRメッセージを受信すると、AAAサーバ(AAAH)1は、上記(4)で抽出したサービスプロファイルを含むHHR(設定要求)メッセージを、移動ノード41を管理するホームエージェント42へ送信する。この処理は、図14のステップS5、S8、S9により実現される。

【0211】(6) HHRメッセージを受信したホームエージェント42は、そのメッセージに含まれているサービスプロファイルに対応する情報をサービス規定データ204に設定する。具体的には、受信したサービスプロファイルをオリジナルサービスプロファイルキャッシュ(OSPC)に設定し、また、移動ノード41のNAIと移動ノード41に割り当てるべきIPv6アドレスとの対応関係を表示するホストアドレス情報をオリジナルホストアドレスキャッシュ(CHAC)に設定する。そして、AAAサーバ(AAAH)1へHHA(設定応答)メッセージを返送する。

【0212】(7)～(9) 実施例3の(7)～(9)と同様に、AAAサーバ(AAAH)1からAAAサーバ(AAAL)2を介してエッジノード22へAHAメッセージが送信され、エッジノード22からIPv6ホスト11へICMP-AA応答メッセージが送信される。ただし、この実施例では、AHAメッセージと共に移動ノード41のサービスプロファイルがエッジノード22に配布される。

【0213】上記シーケンスによれば、モバイルIPv6環境においても、移動ノード41のサービス情報をホームエージェント42および移動ノード11を収容するエッジノード22に配布できる。

#### 実施例5

実施例5は、図4に示したネットワーク構成を前提とする。また、このネットワークでは、階層化モバイルIPv6が適用されているものとする。そして、移動ノード41が外部ドメインにおいてアドレス割当てを要求する際に、AAAサーバ(AAAH)1がホームエージェント42、移動ノード41が位置するドメイン内のモビリティアンカーポイント(MAP)45、および移動ノード41を収容するエッジノード22にサービス情報を配布する。以下、図47を参照しながら、サービス情報の配布シーケンスを説明する。

【0214】(1)～(7)は、実施例4の(1)～(7)と同じである。すなわち、移動ノード41からエッジノード22へICMP-AA要求メッセージが送信され、エッジノード22からAAAサーバ(AAAL)2を介してAAAサーバ(AAAH)1へAHRメッセージが送信される。続いて、AAAサーバ(AAAH)1において、移動ノード41のサービス情報が抽出される。そして、そのサ

ービスプロファイルは、HHRメッセージを利用してホームエージェント42へ配布される。また、AAAサーバ(AAAH)1からAAAサーバ(AAAL)2へ移動ノード41のサービスプロファイルを含むAHAメッセージが送信される。

【0215】(8) AHAメッセージを受信したAAAサーバ(AAAL)2は、そのメッセージから移動ノード41のサービスプロファイルを取得する。そして、そのサービスプロファイルを含むHHRメッセージを作成し、それを同一ドメイン内のモビリティアンカーポイント(MAP)45へ送信する。この処理は、図22のステップS22～S25により実現される。

【0216】(9) HHRメッセージを受信したモビリティアンカーポイント(MAP)45は、実施例4の(6)と同様に、そのメッセージに含まれているサービスプロファイルに対応する情報をサービス規定データ204に設定する。そして、AAAサーバ(AAAH)2へHHAメッセージを返送する。この処理は、図20のステップS7～S74により実現される。

【0217】(10) HHAメッセージを受信したAAAサーバ(AAAH)2は、AAAサーバ(AAAH)1から受信したAHAメッセージをエッジノード22へ回送する。

(11) AHAメッセージを受信したエッジノード22は、移動ノード41のサービスプロファイルを取得すると共に、ICMP-AA応答メッセージを移動ノード41へ送信する。

【0218】上記シーケンスにより、移動ノード41のサービス情報は、移動ノードが位置する外部ドメインに設けられているモビリティアンカーポイント(MAP)45に配布される。

#### 実施例6

実施例6は、図4に示したネットワーク構成を前提とする。また、このネットワークでは、階層化モバイルIPv6が適用されているものとする。また、移動ノード41は、外部ドメインに位置するものとする。そして、移動ノード41がその外部ドメインにおいて結合更新を要求する際に、AAAサーバ(AAAL)2から移動ノード41を管理するモビリティアンカーポイント(MAP)45へサービス情報が配布される。以下、図48を参照しながら、サービス情報の配布シーケンスを説明する。なお、ここでは、AAAL2は、実施例4または実施例5に示したシーケンスにより、移動ノード41のサービス情報を取得しているものとする。

【0219】(1) 移動ノード41は、結合更新(Binding Update)メッセージをモビリティアンカーポイント(MAP)45へ送出する。結合更新メッセージは、移動ノードの位置登録を行うためのメッセージである。

【0220】(2) エッジノード22は、移動ノード41から送出された結合更新メッセージをモビリティアンカーポイント45へ回送する。この処理は、図32のス

ップS162で「No」と判断されることにより実現される。

【0221】(3) モビリティアンカーポイント45は、移動ノード41から結合更新メッセージを受信すると、移動ノード41のRCOA (Regional Care-of-Address) を含むASR (抽出要求) メッセージを作成する。ここで、RCOAは、移動ノードが位置する通信エリアを管理するモビリティアンカーポイントを識別するアドレスである。そして、このASRメッセージは、AAAサーバ (AAAL) 2へ送出される。この処理は、図21のステップS85により実現される。

【0222】(4) ASRメッセージを受信したAAAサーバ (AAAL) 2は、移動ノード41のアドレス割当て時に設定されているサービス規定データ105から、移動ノード41のRCOAに対応するサービスプロファイルを抽出する。この処理は、図16のステップS42～S43により実現される。

【0223】(5) AAAサーバ (AAAL) 2は、上記(4)で抽出したサービスプロファイルをASA (抽出応答) メッセージに格納し、それをモビリティアンカーポイント45へ送出する。この処理は、図16のステップS44により実現される。

【0224】(6) ASAメッセージを受信したモビリティアンカーポイント45は、実施例4の(6)と同様に、そのメッセージに含まれているサービスプロファイルに対応する情報をサービス規定データ204に設定する。

【0225】上記シーケンスによれば、移動ノード41が外部ドメインにおいて結合更新を要求したとき、ホームドメインに設けられているAAAサーバ (AAAH) 1にアクセスすることなく、モビリティアンカーポイントに移動ノード41のサービス情報を配布できる。よって、AAAサーバ (AAAH) 1の負荷が軽くなる。

#### 実施例7

実施例7は、図4に示したネットワーク構成を前提とする。また、このネットワークでは、階層化モバイルIP v6が適用されているものとする。さらに、移動ノード41は、外部ドメインに位置するものとする。そして、移動ノード41がその外部ドメインにおいて結合更新を要求する際に、移動ノード41を収容するエッジノード22がその移動ノード41を管理するモビリティアンカーポイント (MAP) 45にサービス情報を配布する。以下、図49を参照しながら、サービス情報の配布シーケンスを説明する。なお、ここでは、エッジノード22は、実施例4または実施例5に示したシーケンスにより、移動ノード41のサービス情報を取得しているものとする。

【0226】(1) 移動ノード41は、結合更新 (Binding Update) メッセージをモビリティアンカーポイント (MAP) 45へ送出する。

(2) 結合更新メッセージを受信したエッジノード22

は、移動ノード41のアドレス割当て時に設定されているサービス規定データ306から、移動ノード41のサービスプロファイルを抽出する。この処理は、図32のステップS162～164により実現される。

【0227】(3) エッジノード22は、上記(2)で抽出したサービスプロファイルを含む結合更新メッセージを作成し、それをモビリティアンカーポイント45に対して送出する。

【0228】(4) 結合更新メッセージを受信したモビリティアンカーポイント45は、実施例4の(6)と同様に、そのメッセージに含まれているサービスプロファイルに対応する情報をサービス規定データ204に設定する。

【0229】上記シーケンスによれば、AAAサーバにアクセスすることなく、移動ノード41を収容するエッジノード22から、外部ドメイン内で移動ノード41を管理するモビリティアンカーポイント45へ移動ノード41のサービス情報が配布される。

#### 実施例8

実施例8は、図1～図4のいずれかに示したネットワーク構成を前提とする。そして、IP v6ホスト11がエッジノード22に収容されており、IP v6ホスト12がエッジノード21に収容されている。また、IP v6ホスト11のサービスプロファイルおよびホストアドレス情報がエッジノード22に設定されており、IP v6ホスト12のサービスプロファイルおよびホストアドレス情報がエッジノード21に設定されているものとする。なお、IP v6ホストのサービスプロファイルおよびホストアドレス情報をエッジノードに設定する手順は、実施例1、2、4、5において説明した通りである。また、この実施例および後続の実施例9、10において、IP v6ホストは、モバイルIP v6端末を含むものとする。

【0230】上記ネットワークにおいて、IP v6ホスト11からIP v6ホスト12へのパケット送信の開始に際して、送信側ホスト (IP v6ホスト11) を収容するエッジノード22が、受信側ホスト (IP v6ホスト12) を収容するエッジノード21から、受信側ホストのホストアドレス情報および／またはサービスプロファイルを取得する。以下、図50を参照しながら、エッジノード間でIP v6ホストのホストアドレス情報および／またはサービスプロファイルを転送するシーケンスを説明する。

【0231】(1) IP v6ホスト11からIP v6ホスト12へデータパケットが送出される。

(2) 上記データパケットを中継するエッジノード22は、そのパケットの送信元アドレスおよび着信先アドレスがサービス制御データ308のアドレスキャッシュ (ADC) に格納されているか否かを調べる。ここでは、着信先アドレスが格納されていなかったものとする。こ

の場合、エッジノード22は、抽出要求を含むNAI-SPC要求メッセージを作成し、それを上記データパケットの着信先アドレスへ送出する。この処理は、図27のステップS93、S94、S96、S97、図28のステップS114～116、図35のステップS230、図36のステップS246、および図34のステップS212により実現される。

【0232】(3) エッジノード21は、IPv6ホスト12へ向かうNAI-SPC要求メッセージを受信すると、そのメッセージに含まれている抽出要求に従って、サービス規定データ306からIPv6ホスト12のサービスプロファイルおよびホストアドレス情報を抽出する。具体的には、NAI-SPC要求メッセージの着信先アドレスに対応するサービスプロファイルおよびホストアドレス情報を抽出する。この処理は、図31のステップS143～S145、図35のステップS226～S227により実現される。

【0233】(4) エッジノード21は、上記(3)で抽出したIPv6ホスト12のサービスプロファイルおよびホストアドレス情報を含むNAI-SPC応答メッセージを作成し、それをエッジノード22へ送出する。この処理は、図31のステップS146、150により実現される。

【0234】(5) NAI-SPC応答メッセージを受信したエッジノード22は、そのメッセージからIPv6ホスト12のサービスプロファイルおよびホストアドレス情報を抽出し、それらをサービス実行データ307に設定する。この処理は、図33のステップS184、図35のステップS228により実現される。

【0235】上記シーケンスにより、送信側ホストを収容するエッジノードは、受信側ホストを収容するエッジノードからその受信側ホストのサービスプロファイルおよび／またはホストアドレス情報を取得できる。

#### 実施例9

実施例9は、図1～図4のいずれかに示したネットワーク構成を前提とする。また、IPv6ホスト11、12、エッジノード21、22は、実施例8と同じであるものとする。そして、IPv6ホスト11からIPv6ホスト12へのパケット送信の開始に際して、送信側ホスト(IPv6ホスト11)を収容するエッジノード22から受信側ホスト(IPv6ホスト12)を収容するエッジノード21へ送信側ホストのホストアドレス情報が転送される。以下、図51を参照しながら、エッジノード間でIPv6ホストのホストアドレス情報を転送するシーケンスを説明する。

【0236】(1) IPv6ホスト11からIPv6ホスト12へデータパケットが送出される。

(2) 上記データパケットを中継するエッジノード22は、実施例8の(2)と同様の手順でサービス制御データ308のアドレスキャッシュ(ADC)をチェックする。ここでは、送信元アドレスまたは着信先アドレスが格納されていなかったものとする。この場合、エッジノード22は、IPv6ホスト11のサービスプロファイルおよびホストアドレス情報、設定要求、および抽出要求を含むNAI-SPC要求メッセージを作成し、それを上記データパケットの着信先アドレスへ送出する。これら

ここでは、送信元アドレスまたは着信先アドレスが格納されていなかったものとする。この場合、エッジノード22は、IPv6ホスト11のホストアドレス情報および設定要求を含むNAI-SPC要求メッセージを作成し、それを上記データパケットの着信先アドレスへ送出する。これらの処理は、図27のステップS93、S94、S96、S97、図28のステップS111～116、図35のステップS230、図36または図37のシーケンス、および図34のステップS212により実現される。

【0237】(3) エッジノード21は、IPv6ホスト12へ向かうNAI-SPC要求メッセージを受信すると、そのメッセージに含まれているIPv6ホスト11のホストアドレス情報をサービス実行データ307に設定する。この処理は、図31のステップS147、図35のステップS228により実現される。

【0238】上記シーケンスにより、受信側ホストを収容するエッジノードは、送信側ホストを収容するエッジノードからその送信側ホストのホストアドレス情報を取得できる。なお、この実施例では、送信側ホストのホストアドレス情報のみが転送されているが、送信側ホストのサービスプロファイルおよびホストアドレス情報が転送されるようにしてもよい。

#### 実施例10

実施例10は、図1～図4のいずれかに示したネットワーク構成を前提とし、また、IPv6ホスト11、12、エッジノード21、22は、実施例8または9と同じであるものとする。そして、IPv6ホスト11からIPv6ホスト12へのパケット送信の開始に際して、送信側ホスト(IPv6ホスト11)を収容するエッジノード22と受信側ホスト(IPv6ホスト12)を収容するエッジノード21との間でそれぞれが保持しているサービスプロファイルおよびホストアドレス情報が相互に交換される。以下、図52を参照しながら、エッジノード間でIPv6ホストのサービスプロファイルおよびホストアドレス情報を転送するシーケンスを説明する。なお、実施例10のシーケンスは、実施例8および実施例9のシーケンスを組み合わせることにより実現可能である。

【0239】(1) IPv6ホスト11からIPv6ホスト12へデータパケットが送出される。

(2) 上記データパケットを中継するエッジノード22は、実施例8の(2)と同様の手順でサービス制御データ308のアドレスキャッシュ(ADC)をチェックする。ここでは、送信元アドレスまたは着信先アドレスが格納されていなかったものとする。この場合、エッジノード22は、IPv6ホスト11のサービスプロファイルおよびホストアドレス情報、設定要求、および抽出要求を含むNAI-SPC要求メッセージを作成し、それを上記データパケットの着信先アドレスへ送出する。これら

の処理は、図27のステップS93、S94、S96、S97、図28または図29のシーケンス、図35のステップS230、図36または図37のシーケンス、および図34のステップS212により実現される。

【0240】(3) エッジノード21は、IPv6ホスト12へ向かうNAI-SPC要求メッセージを受信すると、そのメッセージに含まれているIPv6ホスト11のサービスプロファイルおよびホストアドレス情報をサービス実行データ307に設定する。また、エッジノード21は、そのメッセージに含まれている抽出要求に従い、サービス規定データ306からIPv6ホスト12のサービスプロファイルおよびホストアドレス情報を抽出する。これらの処理は、図31のステップS143～S150、図35のステップS226～S228により実現される。

【0241】(4)～(5) 実施例8の(4)～(5)と同様に、エッジノード21からエッジノード22へNAI-SPC応答メッセージを利用してIPv6ホスト12のサービスプロファイルおよびホストアドレス情報が転送され、それらがエッジノード22のサービス実行データ307に設定される。このとき、エッジノード22において、必要に応じてサービス規定データ306に保持されているIPv6ホスト11のサービスプロファイルおよびホストアドレス情報がサービス実行データ307に設定される。

【0242】上記シーケンスにより、送信側ホストを収容するエッジノードから受信側ホストを収容するエッジノードへ送信側ホストのサービスプロファイルおよびホストアドレス情報が転送され、また、受信側ホストを収容するエッジノードから送信側ホストを収容するエッジノードへ受信側ホストのサービスプロファイルおよびホストアドレス情報が転送される。これにより、各エッジノードは、通信中のIPv6ホストのサービス情報の中から、最適なサービス情報を個別に選択することができる。

#### 実施例11

実施例11は、図4に示したネットワーク構成を前提とする。そして、移動ノード41がエッジノード22に収容されており、通信ノード(AN)42がエッジノード21に収容されている。また、移動ノード41のサービスプロファイルおよびホストアドレス情報が、ホームエージェント43に設定されているものとする。なお、移動ノード41のサービスプロファイルおよびホストアドレス情報をホームエージェントに設定する手順は、実施例4、5において説明した通りである。

【0243】実施例11では、上記環境下において、通信ノード42から移動ノード41へのパケット送信の開始に際して、受信側ホスト(移動ノード41)を管理するホームエージェント43から送信側ホスト(通信ノード42)を収容するエッジノード21へ受信側ホストの

サービスプロファイルおよびホストアドレス情報が転送される。以下、図53を参照しながら、移動ノードのサービスプロファイルおよびホストアドレス情報を転送するシーケンスを説明する。

【0244】(1) 通信ノード42から移動ノード41へデータパケットが送出される。

(2) 上記データパケットを中継するエッジノード21は、実施例8の(2)と同様に、サービス制御データ308のアドレスキャッシュ(ADC)をチェックし、着信先アドレスが格納されていなかった場合には、抽出要求を含むNAI-SPC要求メッセージを上記データパケットの着信先アドレスへ送出する。なお、上記データパケットの着信先アドレスは移動ノード41なので、このNAI-SPC要求メッセージは、いったん移動ノード41を管理するホームエージェント43へ転送される。

【0245】(3) ホームエージェント43は、上記NAI-SPC要求メッセージを受信すると、そのメッセージに含まれている抽出要求に従って、サービス規定データ204から移動ノード41のサービスプロファイルおよびホストアドレス情報を抽出する。具体的には、NAI-SPC要求メッセージの着信先アドレスに対応するサービスプロファイルおよびホストアドレス情報を抽出する。この処理は、図20のステップS61～S63により実現される。

【0246】(4) ホームエージェント43は、上記(3)で抽出した移動ノード41のサービスプロファイルおよびホストアドレス情報を含むNAI-SPC応答メッセージを作成し、それをエッジノード21へ送出する。この処理は、図20のステップS64、S65により実現される。

【0247】(5) NAI-SPC応答メッセージを受信したエッジノード21は、そのメッセージから移動ノード41のサービスプロファイルおよびホストアドレス情報を抽出し、それらをサービス実行データ307に設定する。この処理は、図33のステップS184、図35のステップS228により実現される。

【0248】上記シーケンスにより、送信側ホストを収容するエッジノードは、受信側ホストのホームエージェントからその受信側ホストのサービスプロファイルおよびホストアドレス情報を取得できる。すなわち、送信側ホストおよび受信側ホストの位置関係によっては、より短い経路でサービスプロファイルおよびホストアドレス情報の転送が可能になる。

#### 実施例12

実施例12は、図4に示したネットワーク構成を前提とする。また、このネットワークには階層化モバイルIPv6が適用されており、移動ノード41の移動先の外部ドメインにモビリティアンカーポイント(MAP)45が設けられている。なお、移動ノード41、通信ノード42、エッジノード21、22については、実施例11と

同じである。

【0249】実施例12では、上記環境下において、通信ノード42から移動ノード41へのパケット送信の開始に際して、受信側ホスト（移動ノード41）を管理するモビリティアンカーポイント45から送信側ホスト（通信ノード42）を収容するエッジノード21へ受信側ホストのサービスプロファイルおよびホストアドレス情報が転送される。以下、図54を参照しながら、移動ノードのサービスプロファイルおよびホストアドレス情報を転送するシーケンスを説明する。

【0250】(1) 通信ノード42から移動ノード41へデータパケットが送出される。

(2)～(5) 基本的には、実施例11の(2)～(5)と同じである。ただし、エッジノード21は、N A I - S P C 要求メッセージの着信先アドレスとして移動ノード41のR C O Aを指定する。このため、このN A I - S P C 要求メッセージは、移動ノード41を管理するモビリティアンカーポイント45へ転送される。そして、このメッセージを受信したモビリティアンカーポイント45が、N A I - S P C 応答メッセージを利用して、移動ノード41のサービスプロファイルおよびホストアドレス情報をエッジノード21へ送信する。

【0251】上記シーケンスにおいても、送信側ホストおよび受信側ホストの位置関係によっては、より短い経路でサービスプロファイルおよびホストアドレス情報の転送が可能になる。

【0252】なお、実施例8～12では、端末装置間でデータ転送が開始されたときに、その送信側端末を収容するエッジノードにおいてアドレスがチェックされ、そのチェック結果に応じてサービスプロファイルの有効化処理が実行されたり、エッジノード間でサービスプロファイルおよび／またはホストアドレス情報が転送されているが、本発明はこれに限定されるものではない。すなわち、例えば、端末装置間でデータ転送が開始されたときに、その受信側端末を収容するエッジノードにおいてアドレスがチェックされ、そのチェック結果に応じて同様の処理が実行される構成であってもよい。

### 実施例13

本実施形態のサービス制御ネットワークでは、上述したように、I P v 6 ホストへのアドレス割当てに際して、そのI P v 6 ホストを収容する通信ノードに対応するサービスプロファイルが配布される。そして、その配布されたサービスプロファイルに基づいて通信サービスが提供される。

【0253】ただし、配布されたサービスプロファイルは、実際に使用される際に有効化される。すなわち、配布されたサービスプロファイルは、I P v 6 ホストによる通信の開始時に有効化される。具体的には、I P v 6 ホストからパケットを受信したエッジノードは、まず、そのパケットの送信元アドレスおよび着信先アドレスに

基づいて、提供すべきサービスを認識する。続いて、そのサービスを過去に提供したことがあるか否かを調べる。そして、そのサービスを過去に提供したことがあれば、先に使用しサービスプロファイルに従ってそのサービスを提供する。一方、そのサービスを過去に提供したことがない場合には、対応するサービスプロファイルを有効化することにより、そのサービスを提供するためのポリシーテーブルを生成する。

【0254】このように、エッジノードは、過去に提供したことのないサービスを要求されたときは、そのサービスに対応するサービスプロファイル用意し、それを有効化する必要がある。ここで、各サービスは、基本的に、パケットの送信元アドレスおよび着信先アドレスにより特定される。したがって、あるサービスを過去に提供したことがあるか否かは、そのサービスに対応する送信元アドレスおよび着信先アドレスを持ったパケットを過去に受信したか否かを調べることにより認識できる。

【0255】このため、エッジノードは、過去に受信したパケットの送信元アドレスおよび着信先アドレスをアドレスキャッシュに格納する機能、I P v 6 ホストからパケットを受信したときにそのパケットの送信元アドレスおよび着信先アドレスがアドレスキャッシュに格納されているか否かを調べる機能、およびそれらのアドレス格納されていなかった場合に対応するサービスプロファイルを有効化する機能を備えている。

【0256】実施例13では、上記構成のエッジノードにおいて、受信パケットの送信元アドレスがアドレスキャッシュに格納されていなかった場合に、そのパケットに対応するサービスプロファイル有効化するシーケンスを示す。なお、アドレスキャッシュは、図25(a)および図25(b)に示すように、送信側アドレスおよび受信側アドレスを個別に管理する構成である。また、受信パケットの送信元アドレスがアドレスキャッシュに格納されていなかった場合を、「送信側キャッシュミス」と呼ぶこととする。以下、図55を参照しながら、実施例13の有効化シーケンスを説明する。

【0257】(1) ネットワークインターフェース301は、ネットワークから受信したパケットをサービス制御部302に送出する。

(2) サービス制御部302は、受信パケットの送信側アドレス（送信元アドレス）および受信側アドレス（着信先アドレス）がサービス制御データ308内のアドレスキャッシュ(ADC)に格納されているか否かをチェックする。この処理は、図27のステップS93、図28のシーケンスにより実現される。

【0258】(3) 上記(2)において、送信側アドレスまたは受信側アドレスの少なくとも一方が格納されていなかった場合には、サービス制御部302は、上記パケットをプロトコル制御部304に送る。この処理は、図27のステップS96により実現される。なお、この実施

例では、送信側アドレスがアドレスキャッシュに格納されていなかったものとする。すなわち、送信側ヒットミスが発生したものとする。この場合、このアドレスは、アドレスキャッシュに書き込まれる。

【0259】(4) サービス制御部302は、サービスデータ管理部305へヒットミス通知を送る。このヒットミス通知は、送信側ヒットミスが発生したことを表示する情報、および対応するIPv6アドレスを含んでいる。この処理は、図27のステップS97、図28のステップS113により実現される。

【0260】(5) プロトコル制御部304は、サービス制御部302から受け取ったパケットに対して一般的なルーティング処理を行い、ネットワークインターフェース301へ送る。この処理は、図33のステップS203に相当する。

【0261】(6) サービスデータ管理部305は、上記ヒットミス通知を受信すると、サービス規定データ306から、上記パケットの送信側ホストに対応するホストアドレス情報(HA)、およびサービスプロファイルを抽出する。この処理は、図35のステップS230、図36のステップS242により実現される。

【0262】(7) サービスデータ管理部305は、上記(6)で抽出した情報をサービス実行データ307に設定する。そして、サービス実行データ307に格納されているサービスプロファイルのなかで、送信側ホストが上記ヒットミスに対応するIPv6ホストであり、且つ、受信側ホストが当該エッジノードの配下の任意のIPv6ホストと通信中のIPv6ホストである通信のサービスプロファイルのサービス実行状態を「有効」にする。この処理は、図36のステップS243により実現される。

【0263】(8) サービスデータ管理部305は、上記(7)で有効化したサービスプロファイルを、サービス制御データ308内のポリシーテーブルに書き込む。上記シーケンスによれば、送信側ヒットミスが発生すると、そのヒットミスに対応するサービスプロファイルが当該エッジノード内のサービス規定データ306から抽出され、さらにそのサービスプロファイルが有効化されることにより、ポリシーテーブルが生成される。よって、以降は、そのポリシーテーブルによりサービスが提供される。

#### 実施例14

実施例14では、受信パケットの着信先アドレスがアドレスキャッシュに格納されていなかった場合に、そのパケットに対応するサービスプロファイル有効化するシーケンスを示す。なお、アドレスキャッシュは、送信側アドレスおよび受信側アドレスを個別に管理する構成であるものとする。また、受信パケットの送信元アドレスがアドレスキャッシュに格納されていなかった場合を、「受信側キャッシュミス」と呼ぶことにする。以下、図

56を参照しながら、実施例14の有効化シーケンスを説明する。

【0264】(1) ネットワークインターフェース301は、ネットワークから受信したパケットをサービス制御部302に送出する。

(2) サービス制御部302は、実施例13の(2)と同様に、サービス制御データ308内のアドレスキャッシュ(ADC)をチェックする。

【0265】(3) ここでは、受信側アドレスがアドレスキャッシュに格納されていなかったものとする。すなわち、受信側ヒットミスが発生したものとする。この場合、サービス制御部302は、実施例14の(3)と同様に、上記パケットをプロトコル制御部304に送る。また、このアドレスは、アドレスキャッシュに書き込まれる。

【0266】(4) サービス制御部302は、サービスデータ管理部305へヒットミス通知を送る。このヒットミス通知は、受信側ヒットミスが発生したことを表示する情報、および対応するIPv6アドレスを含んでいる。この処理は、図27のステップS97、図28のステップS116により実現される。

【0267】(5) プロトコル制御部304は、実施例13の(5)と同様に、上記パケットをネットワークインターフェース301へ送る。

(6) サービスデータ管理部305は、上記ヒットミス通知を受信すると、必要に応じて、サービス規定データ306から上記パケットの送信側ホストに対応するホストアドレス情報および/またはサービスプロファイルを抽出する。なお、上記情報を抽出する場合とは、例えば、図51または図52に示したように、受信側ホストを収容するエッジノードにホストアドレス情報および/またはサービスプロファイルを転送する場合である。この処理は、図35のステップS230により実現される。

【0268】(7) サービスデータ管理部305は、プロトコル制御部304にパケット生成要求を送る。この処理は、図36のステップS246により実現される。

(8) プロトコル制御部304は、パケット生成要求に従って、N A I - S P C要求メッセージを作成し、それをネットワークインターフェース301へ送る。このメッセージは、受信側ホストのホストアドレス情報および/またはサービスプロファイルをその受信側ホストを収容するエッジノードに要求する抽出要求を含んでいる。また、上記(6)で送信側ホストのホストアドレス情報および/またはサービスプロファイルが抽出された場合は、このメッセージは、それらの抽出された情報も含んでいる。この処理は、図34のステップS212により実現される。

【0269】上記N A I - S P C要求メッセージが送出されると、受信側ホストを収容するエッジノードは、図31のステップS144～S146、図35のS226

～S227を実行することにより、対応するN A I - S P C応答メッセージを返送する。ここで、このN A I - S P C応答メッセージは、受信側ホストのホストアドレス情報および／またはサービスプロファイルを含んでいる。

【0270】(9) ネットワークインターフェース301は、上記N A I - S P C応答メッセージを含むパケットを受信すると、それをサービス制御部302に送る。

(10) サービス制御部302は、上記パケットの宛先が当該エッジノードであることを検出すると、そのパケットをプロトコル制御部304に送る。この処理は、図23のステップS98により実現される。

【0271】(11) プロトコル制御部304は、受信したN A I - S P C応答メッセージに従って、サービスデータ管理部305に設定要求を送る。この設定要求は、N A I - S P C応答メッセージを利用して送られてきた情報をサービス実行データ307に設定することを要求する。この処理は、図33のステップS184により実現される。

【0272】(12) サービスデータ管理部305は、設定要求に従い、受信側ホストのホストアドレス情報および／またはサービスプロファイルをサービス実行データ307に設定する。そして、サービス実行データ307に格納されているサービスプロファイルのなかで、送信側ホストが当該エッジノードの配下の通信中のI Pv6ホストであり、且つ、受信ホストが上記ヒットミスに対応するI Pv6ホストである通信のサービスプロファイルのサービス実行状態を「有効」にする。

【0273】(13) サービスデータ管理部305は、上記(12)で有効化したサービスプロファイルを、サービス制御データ308内のポリシーテーブルに書き込む。

上記シーケンスによれば、受信側ヒットミスが発生すると、受信側ホストを収容するエッジノードから所定の情報を取得し、その情報をを利用して対応するサービスプロファイルを有効化する。よって、以降は、その有効化されたサービスプロファイルに従ってサービスが提供される。

#### 実施例15

実施例15では、受信パケットの送信元アドレスおよび着信先アドレスの双方がアドレスキャッシュに格納されていなかった場合に、対応するサービスプロファイル有効化するシーケンスを示す。なお、アドレスキャッシュは、送信側アドレスおよび受信側アドレスを個別に管理する構成であるものとする。図57に実施例15のシーケンスを示す。

【0274】実施例15のシーケンスは、基本的に、実施例13および実施例14の処理を組み合わせることにより実現される。よって、ここでは、実施例15についての詳細な説明は省略する。ただし、実施例15では、サービス制御部302からサービスデータ管理部305

へ送られるヒットミス通知の中に、送信側ヒットミスおよび受信側ヒットミスの双方が発生したことを表示する情報が格納される。

#### 実施例16

実施例16では、アドレスキャッシュは、図26(a)に示すように、送信側アドレスおよび受信側アドレスの組合せを管理する構成である。そして、受信パケットの送信元アドレスと着信先アドレスの組合せがアドレスキャッシュに格納されていなかった場合には、そのパケットに対応するサービスプロファイルが有効化される。以下、図58を参照しながら、実施例16の有効化シーケンスを説明する。

【0275】(1)～(2) 実施例13の(1)～(2)の同様に、サービス制御データ308のアドレスキャッシュ(ADC)がチェックされる。ただし、実施例16では、受信パケットの送信側アドレスと受信側アドレスの組合せがアドレスキャッシュに格納されているか否かが調べられる。そして、ここでは、そのような組合せが格納されていなかったものとする。

【0276】以降の処理は、基本的に、実施例14の(3)～(13)と同じである。すなわち、当該エッジノードは、受信側ホストを収容するエッジノードへN A I - S P C要求メッセージを送出し、N A I - S P C応答メッセージを受信することにより対応するホストアドレス情報およびサービスプロファイルを取得し、それらをサービス実行データ307およびサービス制御データ308に設定する。

#### 実施例17

本実施形態のサービス制御ネットワークでは、各I Pv6ホストに割り当てられるI Pv6アドレスに対して所定のライフタイムが設定される。そして、あるI Pv6アドレスのライフタイムが消滅すると、そのアドレスに対応するサービス情報が無効化される。すなわち、あるI Pv6ホストのサービス情報がエッジノードに設定されている場合に、そのI Pv6アドレスのライフタイムが消滅すると、対応するサービス情報が削除または無効化される。

【0277】実施例17では、あるサービスの送信側アドレスとして管理されているI Pv6アドレスのライフタイムが消滅した場合に、そのアドレスに対応するサービス情報が無効化される。なお、アドレスキャッシュは、送信側アドレスおよび受信側アドレスを個別に管理する構成であるものとする。以下、図59を参照しながら、実施例17の無効化シーケンスを説明する。

【0278】(1) サービス制御部302は、定期的に、アドレスキャッシュ(ADC)に格納されているすべての送信側ホストアドレスおよび受信側ホストアドレスのライフタイム(有効時間)をデクリメントする。そして、ライフタイムが消滅したアドレスの有無をモニタする。この処理は、図27のステップS99により実現され

る。

【0279】(2) ここでは、ある送信側アドレスのライフタイムが消滅したものとする。すなわち、送信側ライフタイムオーバーが発生したものとする。この場合、サービス制御部302は、サービスデータ管理部305へライフタイムオーバー通知を送る。なお、この通知は、送信側アドレスタイムオーバーが発生したことを表示する情報、およびライフタイムが消滅したアドレスを含んでいる。この処理は、図27のステップS101により実現される。

【0280】(3) サービスデータ管理部305は、サービス制御データ308内の送信側アドレスキャッシング(SAC)およびポリシーテーブル(PT)において、上記アドレスに対応する全てのデータを削除する。この処理は、図35のステップS231、図41のステップS282により実現される。

【0281】(4) サービスデータ管理部305は、サービス実行データ307内の送信側サービスプロファイルキャッシング(SSPC)および送信側ホストアドレスキャッシング(SHAC)において、上記アドレスに対応する全てのデータを削除する。また、受信側サービスプロファイルキャッシング(DSPC)において、上記アドレスに対して有効状態のデータが存在すれば、これを無効状態に変更する。この処理は、図41のステップS283、S284により実現される。

【0282】上記シーケンスによれば、IPv6アドレスのライフタイムが消滅すると、対応するサービス情報が削除／無効化される。すなわち、一定期間以上使用されていないサービス情報は、サービス実行データ307およびサービス制御データ308から削除される。このため、サービス実行データ307およびサービス制御データ308のメモリ領域が効率的に利用される。

【0283】なお、IPv6アドレスのライフタイムの消滅に起因して上記無効化シーケンスが行われた後、そのIPv6アドレスが設定されたパケットを受信すると、アドレスヒットミスが発生し、上述の有効化処理が実行されるので、再びサービスが提供されるようになる。

#### 実施例18

実施例18では、あるサービスの受信側アドレスとして管理されているIPv6アドレスのライフタイムが消滅した場合に、そのアドレスに対応するサービス情報が無効化される。なお、アドレスキャッシングは、送信側アドレスおよび受信側アドレスを個別に管理する構成であるものとする。以下、図60を参照しながら、実施例18の無効化シーケンスを説明する。

【0284】(1) サービス制御部302は、実施例17の(1)と同様に、アドレスキャッシングに格納されている各アドレスのライフタイムをデクリメントすると共に、ライフタイムが消滅したアドレスの有無をモニタする。

【0285】(2) ここでは、ある受信側アドレスのライフタイムが消滅したものとする。すなわち、受信側ライフタイムオーバーが発生したものとする。この場合、サービス制御部302は、サービスデータ管理部305へライフタイムオーバー通知を送る。なお、この通知は、受信側アドレスタイムオーバーが発生したことを表示する情報、およびライフタイムが消滅したアドレスを含んでいる。この処理は、図27のステップS101により実現される。

【0286】(3) サービスデータ管理部305は、サービス制御データ308内の受信側アドレスキャッシング(DAC)およびポリシーテーブル(PT)において、上記アドレスに対応する全てのデータを削除する。この処理は、図35のステップS231、図41のステップS286により実現される。

【0287】(4) サービスデータ管理部305は、サービス実行データ307内の送信側サービスプロファイルキャッシング(SSPC)、送信側ホストアドレスキャッシング(SHAC)、受信側サービスプロファイルキャッシング(DSPC)、受信側ホストアドレスキャッシング(DHAC)において、上記アドレスに対応するすべてのデータを削除する。この処理は、図41のステップS287、S288により実現される。

#### 実施例19

実施例19は、アドレスキャッシングにおいて送信側アドレスおよび受信側アドレスの組合せが管理されることを前提とする。そして、ある送信側アドレスおよび受信側アドレスの組合せに対して設定されているライフタイムが消滅した場合に、その組合せに対応するサービス情報が無効化される。以下、図61を参照しながら、実施例19の無効化シーケンスを説明する。

【0288】(1) サービス制御部302は、定期的に、アドレスキャッシングに格納されている送信側ホストアドレスと受信側ホストアドレスとの各組合せに対して設定されているライフタイムをデクリメントする。そして、ライフタイムが消滅した組合せの有無をモニタする。

【0289】(2) ここでは、ある組合せのライフタイムが消滅したものとする。即ち、ライフタイムオーバーが発生したものとする。この場合、サービス制御部302は、サービスデータ管理部305へライフタイムオーバー通知を送る。なお、この通知は、アドレスタイムオーバーが発生したことを表示する情報、およびライフタイムの消滅に係わる送信側アドレスおよび受信側アドレスを含んでいる。

【0290】(3) サービスデータ管理部305は、サービス制御データ308内のアドレスキャッシング(ADC)およびポリシーテーブル(PT)において、上記送信側アドレスおよび受信側アドレスに係わるデータを削除する。この処理は、図35のステップS231、図41に示す処理により実現される。

【0291】(4) サービスデータ管理部305は、サービス実行データ307内の送信側サービスプロファイルキャッシュ(SSPC)、送信側ホストアドレスキャッシュ(SHAC)、受信側サービスプロファイルキャッシュ(DSPC)、受信側ホストアドレスキャッシュ(DHAC)において、ライフタイムオーバーに係わる送信側ホストおよび受信側ホストが他のIPv6ホストと通信中でなければ、対応する情報を削除する。一方、ライフタイムオーバーに係わる送信側ホストおよび受信側ホストが他のIPv6ホストを通信中であった場合は、対応する情報を無効化する。これらの処理は、図42に示す処理により実現される。

#### 実施例20

実施例17～19では、IPv6アドレスに対して設定されているライフタイムの消滅に起因して対応するサービス情報の無効化が行われている。これに対して、実施例20では、端末(IPv6ホスト、移動ノード)からの要求により、エッジノードに設定されているサービス情報が無効化される。具体的には、IPv6ホストからセッション解放要求が送出されたときに、そのIPv6ホストを収容するエッジノードにおいて対応するサービス情報が無効化／削除される。以下、図62を参照しながら実施例20のシーケンスを説明する。

【0292】(1) IPv6ホスト11は、そのIPv6ホスト11を収容しているエッジノード21に対し、AAA-Teardown要求メッセージを送出する。尚、IPv6ホスト11は、例えば、通信の終了時にこのメッセージを送出するものとする。

【0293】(2) エッジノード21は、上記AAA-Teardown要求メッセージの送信元であるIPv6ホスト11のセッションを管理するAAAサーバ1へSTR(削除要求)メッセージを送出する。この処理は、図33のステップS202により実現される。

【0294】(3) AAAサーバ1は、STRメッセージを受信すると、IPv6ホスト11に係わるセッション情報を削除する。この処理は、図14のステップS12により実現される。

【0295】(4) AAAサーバ1は、STRメッセージの送信元であるエッジノード21へSTA(削除応答)メッセージを送出する。この処理は、図14のステップS13により実現される。

【0296】(5) エッジノード21は、STAメッセージを受信すると、セッションが解放されたIPv6ホスト11に対して適用されているサービスを無効化し、そのIPv6ホスト11に対応するホストアドレス情報およびサービスプロファイルを削除する。この処理は、図32のステップS172、図35のステップS229により実現される。

【0297】(6) エッジノード21は、IPv6ホスト11へAAA-Teardown応答メッセージを送出する。こ

の処理は、図32のステップS176により実現される。

#### 実施例21

実施例21では、実施例20と同様に、端末からの要求によりその端末を収容するエッジノードにおいて対応するサービス情報が削除／無効化される。これに加えて、実施例21では、上記サービス情報が当該エッジノードから他の通信ノードに配布されていた場合に、その通信ノードにおいても同様にサービス情報が削除／無効化される。以下、図63を参照しながら実施例21のシーケンスを説明する。

【0298】なお、この実施例では、IPv6ホスト11は、IPv6ホスト12と通信をしていたものとする。また、IPv6ホスト11はエッジノード21に収容されており、IPv6ホスト12はエッジノード22に収容されているものとする。さらに、上記通信の開始に際して、エッジノード21からエッジノード22へIPv6ホスト11のサービス情報が転送されたものとする。

【0299】(1)～(4) 実施例20の(1)～(4)と同じである。

(5) エッジノード21は、STAメッセージを受信すると、実施例20の(5)と同様に、IPv6ホスト11に対応するホストアドレス情報およびサービスプロファイルを削除する。

【0300】(6) エッジノード21は、IPv6ホスト11の通信相手であったIPv6ホスト12に対してNAT-SPC要求メッセージを送る。このメッセージは、IPv6ホスト11のIPv6アドレスおよび削除要求を含んでいる。なお、この処理は、図32のステップS175により実現される。

【0301】(7) エッジノード22は、IPv6ホスト12宛のNAT-SPC要求メッセージを受信すると、IPv6ホスト11に係わるサービスを無効化する。さらに、IPv6ホスト11との通信に係わるサービスのためにエッジノード21から受信したホストアドレス情報およびサービスプロファイルを、それぞれ受信側ホストアドレスキャッシュ(DHAC)および受信側サービスプロファイルキャッシュ(DSPC)から除する。この処理は、図31のステップS147、図35のステップS229により実現される。

【0302】(8) エッジノード22は、IPv6ホスト11のIPv6アドレスを含むNAT-SPC応答メッセージをエッジノード21へ送出する。この処理は、図31のステップS149により実現される。

【0303】(9) エッジノード21は、NAT-SPC応答メッセージを受信すると、IPv6ホスト11へAAA-Teardown応答メッセージを送出する。この処理は、図33のステップS183により実現される。

【0304】なお、上記実施例では、エッジノード21

がその通信相手であった I Pv6 ホスト 12 に対して NAI-SPC 要求メッセージを送ることにより、エッジノード 22 が NAI-SPC 要求メッセージを受信しているが、他の方法も考えられる。例えば、エッジノードは、IPv6 ホストのサービス情報を他の通信ノードへ配布したときに、その送り先アドレスを図 13 (b) に示すオリジナルホストアドレスキャッシュの「送出先 IPv6 アドレス」に格納しておけば、上記 (6) において送出される NAI-SPC 要求メッセージを直接的に送り先を認識することができる。

(付記 1) 端末装置を収容するルータ装置および上記端末装置を認証するサーバ装置を備え、上記端末装置に対してサービスを提供するサービス制御ネットワークであって、上記ルータ装置は、上記端末装置からアドレス要求を受信したときに、上記サーバ装置に対して認証要求を送出する要求手段と、上記サーバ装置から上記認証要求に対応する認証応答および上記端末装置のサービス情報を受信し、そのサービス情報に従ってサービスを提供する提供手段と、上記端末装置に対して上記アドレス要求に対応するアドレス応答を送出する応答手段とを有し、上記サーバ装置は、上記認証要求に基づいて上記端末装置を認証し、上記認証要求に対応する認証応答および上記端末装置のサービス情報を上記ルータ装置へ送出する送出手段を有することを特徴とするサービス制御ネットワーク。

【0305】(付記 2) 端末装置を収容するルータ装置および上記端末装置を認証するサーバ装置を備え、上記端末装置に対してサービスを提供するサービス制御ネットワークであって、上記ルータ装置は、上記端末装置から ICMPv6 によるアドレス要求を受信したときに、上記サーバ装置に対して AAA プロトコルによる認証要求を送出する要求手段と、上記サーバ装置から上記認証要求に対応する認証応答および上記端末装置のサービス情報を受信し、そのサービス情報に従ってサービスを提供する提供手段と、上記端末装置に対して上記アドレス要求に対応するアドレス応答を送出する応答手段とを有し、上記サーバ装置は、上記認証要求に基づいて上記端末装置を認証し、上記認証要求に対応する認証応答および上記端末装置のサービス情報を上記ルータ装置へ送出する送出手段を有することを特徴とするサービス制御ネットワーク。

【0306】(付記 3) 付記 2 に記載のサービス制御ネットワークであって、上記端末装置が外部ドメインから上記アドレス要求を送出したときに、上記サーバ装置は、上記端末装置のホームドメインと上記外部ドメインとの間に設けられるゲートウェイ装置へ上記サービス情報を配布する。

【0307】(付記 4) 付記 2 に記載のサービス制御ネットワークであって、上記サーバ装置は、階層化モバイル IPv6 において規定されているモビリティアンカー

ポイントへ上記サービス情報を配布する。

【0308】(付記 5) 端末装置を収容するルータ装置および上記端末装置を認証するサーバ装置を備えるサービス制御ネットワークにおいて、上記端末装置に提供すべきサービスを規定するサービス情報を上記ルータ装置へ配布するサービス情報配布方法であって、上記端末装置から上記ルータ装置へ ICMPv6 によるアドレス要求が送出され、上記ルータ装置から上記サーバ装置へ AAA プロトコルによる認証要求が送出され、上記サーバ装置により上記端末装置が認証され、上記サーバ装置から上記ルータ装置へ上記認証要求に対応する認証応答および上記端末装置のサービス情報が送出され、上記ルータ装置から上記端末装置へ上記アドレス要求に対応するアドレス応答が送出されるを特徴とするサービス情報配布方法。

【0309】(付記 6) 端末装置を収容するルータ装置および上記端末装置を認証するサーバ装置を備えるサービス制御ネットワークにおいて使用されるルータ装置であって、上記端末装置から ICMPv6 によるアドレス要求を受信したときに、上記サーバ装置に対して AAA プロトコルによる認証要求を送出する要求手段と、上記サーバ装置から上記認証要求に対応する認証応答および上記端末装置のサービス情報を受信し、その受信したサービス情報に従ってサービスを提供する提供手段と、上記端末装置に対して上記アドレス要求に対応するアドレス応答を送出する応答手段とを有することを特徴とするルータ装置。

【0310】(付記 7) 第 1 の端末装置を収容する第 1 のルータ装置、第 2 の端末装置を収容する第 2 のルータ装置、および上記第 1 および第 2 の端末装置に提供すべきサービスを規定するサービス情報を管理するサーバ装置を備え、上記第 1 および第 2 の端末装置にサービスを提供するサービス制御ネットワークであって、上記第 1 のルータ装置に設けられ、上記第 1 の端末装置に提供すべきサービスを規定するサービス情報を上記サーバ装置から受信して保持する第 1 の保持手段と、上記第 2 のルータ装置に設けられ、上記第 2 の端末装置に提供すべきサービスを規定するサービス情報を上記サーバ装置から受信して保持する第 2 の保持手段と、上記第 1 の端末装置と上記第 2 の端末装置との間の通信の開始を契機として、上記第 1 のルータ装置と上記第 2 のルータ装置との間で対応するサービス情報を転送する転送手段と、上記第 1 の保持手段に保持されているサービス情報、上記第 2 の保持手段に保持されているサービス情報、および上記転送手段により転送されたサービス情報の少なくとも一部を利用してサービスを提供する提供手段と、を有することを特徴とするサービス制御ネットワーク。

【0311】(付記 8) 第 1 の端末装置を収容する第 1 のルータ装置、第 2 の端末装置を収容する第 2 のルータ装置、および上記第 1 および第 2 の端末装置に提供すべ

きサービスを規定するサービス情報を管理するサーバ装置を備え、上記第1および第2の端末装置にサービスを提供するサービス制御ネットワークであって、上記第1のルータ装置に設けられ、上記第1の端末装置に提供すべきサービスを規定するサービス情報を上記サーバ装置から受信して保持する第1のサービス情報保持手段と、上記第1のルータ装置に設けられ、上記第1の端末装置に設定されているネットワークアクセス識別子と上記第1の端末装置に動的に割り当てるアドレスとの対応関係を表すアドレス情報を保持する第1のアドレス情報保持手段と、上記第2のルータ装置に設けられ、上記第2の端末装置に提供すべきサービスを規定するサービス情報を上記サーバ装置から受信して保持する第2のサービス情報保持手段と、上記第2のルータ装置に設けられ、上記第2の端末装置に設定されているネットワークアクセス識別子と上記第2の端末装置に動的に割り当てるアドレスとの対応関係を表すアドレス情報を保持する第2のアドレス情報保持手段と、上記第1の端末装置と上記第2の端末装置との間の通信の開始を契機として、上記第1のルータ装置と上記第2のルータ装置との間で対応するアドレス情報、あるいはアドレス情報とサービス情報を転送する転送手段と、上記第1のサービス情報保持手段に保持されているサービス情報、上記第2のサービス情報保持手段に保持されているサービス情報、上記第1のアドレス情報保持手段に保持されているアドレス情報、上記第2のアドレス情報保持手段に保持されているアドレス情報、および上記転送手段により転送された情報の少なくとも一部を利用してサービスを提供する提供手段と、を有することを特徴とするサービス制御ネットワーク。

【0312】(付記9)付記8に記載のサービス制御ネットワークであって、上記サービス情報は、それぞれ対応する端末装置のネットワークアクセス識別子を利用して管理されている。

【0313】(付記10)付記9に記載のサービス制御ネットワークであって、上記第1の端末装置から上記第2の端末装置へパケットが送出されたときに、上記第1および第2のアドレス情報保持手段のうちの少なくとも一方により保持されているアドレス情報をを利用して、上記パケットの送信側アドレスおよび受信側アドレスに対応するネットワークアクセス識別子を検出し、その検出されたネットワークアクセス識別子に対応するサービス情報をを利用してサービスが提供される。

【0314】(付記11)付記9に記載のサービス制御ネットワークであって、上記第1のルータ装置は、上記第1の端末装置から上記第2の端末装置へパケットが送出されたときに、そのパケットの送信側アドレスに対応するネットワークアクセス識別子を検出し、その検出されたネットワークアクセス識別子に対応するサービス情報を有効化する。

【0315】(付記12)付記9に記載のサービス制御ネットワークであって、上記第1のルータ装置は、上記第1の端末装置から上記第2の端末装置へパケットが送出されたときに、そのパケットの受信側アドレスに対応するアドレス情報を上記第2のルータ装置に要求し、上記第2のルータ装置は、上記要求に応じて、上記第2の端末装置のアドレス情報を上記第1のルータ装置へ送出する。

【0316】(付記13)付記9に記載のサービス制御ネットワークであって、上記第1のルータ装置が備える第1のサービス情報保持手段には上記第2の端末装置のサービス情報が保持されており、上記第1のルータ装置は、上記第1の端末装置から上記第2の端末装置へパケットが送出されたときに、そのパケットの受信側アドレスに対応するアドレス情報を上記第2のルータ装置に要求し、上記第2のルータ装置は、上記要求に応じて、上記第2の端末装置のアドレス情報を上記第1のルータ装置へ送出する。

【0317】(付記14)付記9に記載のサービス制御ネットワークであって、上記第1のルータ装置が備える第1のサービス情報保持手段には上記第2の端末装置のサービス情報が保持されており、上記第1のルータ装置は、上記第1の端末装置から上記第2の端末装置へパケットが送出されたときに、そのパケットの受信側アドレスに対応するアドレス情報を上記第2のルータ装置に要求し、上記第2のルータ装置は、上記要求に応じて、上記第2の端末装置のアドレス情報を上記第1のルータ装置へ送出し、上記第1のルータ装置は、上記第1のサービス情報保持手段に保持されている上記第2の端末装置のサービス情報と上記第2のルータ装置から送出された上記第2の端末装置のサービス情報をマージする。

【0318】(付記15)付記9に記載のサービス制御ネットワークであって、上記第1のルータ装置は、上記第1の端末装置から上記第2の端末装置へパケットが送出されたときに、そのパケットの送信側アドレスに対応するアドレス情報を上記第2のルータ装置へ送出し、上記第2のルータ装置は、受信したアドレス情報を上記第2のルータ装置へ送出する。

【0319】(付記16)付記9に記載のサービス制御ネットワークであって、上記第2のルータ装置が備える第2のサービス情報保持手段には上記第1の端末装置のサービス情報が保持されており、上記第1のルータ装置は、上記第1の端末装置から上記第2の端末装置へパケットが送出されたときに、そのパケットの受信側アドレスに対応するアドレス情報を上記第2のルータ装置へ送出し、上記第2のルータ装置は、受信したアドレス情報を上記第2のルータ装置へ送出する。

【0320】(付記17)付記9に記載のサービス制御

ネットワークであって、上記第1のルータ装置は、受信したパケットの送信側アドレスおよび受信側アドレスを個別に管理するアドレスキャッシュと、新たに受信したパケットの送信側アドレスまたは受信側アドレスが上記アドレスキャッシュに格納されていなかった場合に、対応するサービス情報を有効化する手段とを有する。

【0321】(付記18)付記9に記載のサービス制御ネットワークであって、上記第1のルータ装置は、受信したパケットの送信側アドレスと受信側アドレスとの組合せを管理するアドレスキャッシュと、新たに受信したパケットの送信側アドレスと受信側アドレスとの組合せが上記アドレスキャッシュに格納されていなかった場合に、対応するサービス情報を有効化する手段とを有する。

【0322】(付記19)付記9に記載のサービス制御ネットワークであって、上記第1のルータ装置は、受信したパケットの送信側アドレスおよび受信側アドレスのライフタイムを個別に管理するアドレスキャッシュと、上記アドレスキャッシュにより管理されているアドレスのライフタイムが消滅したときに、対応するアドレス情報およびサービス情報を削除または無効化する手段とを有する。

【0323】(付記20)付記9に記載のサービス制御ネットワークであって、上記第1のルータ装置は、受信したパケットの送信側アドレスと受信側アドレスとの組合せを管理するアドレスキャッシュと、上記アドレスキャッシュにより管理されているアドレスの組合せのライフタイムが消滅したときに、対応するアドレス情報およびサービス情報を削除または無効化する手段とを有する。

【0324】(付記21)付記9に記載のサービス制御ネットワークであって、上記第1のルータ装置は、上記第1の端末装置からの要求に従って、その第1の端末装置に対応するアドレス情報およびサービス情報を削除または無効化する手段をさらに有する。

【0325】(付記22)付記9に記載のサービス制御ネットワークであって、上記第1のルータ装置は、上記第1の端末装置からの要求に従って、上記第2のルータ装置に設定されている上記第1の端末装置に対応するアドレス情報およびサービス情報を削除または無効化する手段をさらに有する。

【0326】(付記23)第1の端末装置を収容する第1のルータ装置、第2の端末装置を収容する第2のルータ装置、および上記第1および第2の端末装置に提供すべきサービスを規定するサービス情報を管理するサーバ装置を備えるサービス制御ネットワークにおいて、上記第1および第2の端末装置にサービスを提供するサービス提供方法であって、上記サーバ装置から上記第1のルータ装置へ上記第1の端末装置に提供すべきサービスを規定するサービス情報を配布し、上記第1のルータ装置

において、上記第1の端末装置に設定されているネットワークアクセス識別子と上記第1の端末装置に動的に割り当てるアドレスとの対応関係を表すアドレス情報を生成し、上記サーバ装置から上記第2のルータ装置へ上記第2の端末装置に提供すべきサービスを規定するサービス情報を配布し、上記第2のルータ装置において、上記第2の端末装置に設定されているネットワークアクセス識別子と上記第2の端末装置に動的に割り当てるアドレスとの対応関係を表すアドレス情報を生成し、上記第1の端末装置と上記第2の端末装置との間の通信の開始を契機として、上記第1のルータ装置と上記第2のルータ装置との間で対応するアドレス情報、あるいはアドレス情報とサービス情報を転送し、上記サーバ装置から上記第1のルータ装置に配布されたサービス情報、上記サーバ装置から上記第2のルータ装置に配布されたサービス情報、上記第1ルータ装置において生成されたアドレス情報、上記第2ルータ装置において生成されたアドレス情報、および第1のルータ装置と第2のルータ装置との間で転送された情報の少なくとも一部を利用してサービスを提供することを特徴とするサービス提供方法。

【0327】(付記24)第1の端末装置を収容する第1のルータ装置、第2の端末装置を収容する第2のルータ装置、および上記第1および第2の端末装置に提供すべきサービスを規定するサービス情報を管理するサーバ装置を備えるサービス制御ネットワークにおいて、上記第1のルータ装置として使用されるルータ装置であって、上記第1の端末装置に提供すべきサービスを規定するサービス情報を上記サーバ装置から受信し、上記第1の端末装置に設定されているネットワークアクセス識別子と関連づけてそのサービス情報を保持するサービス情報保持手段と、上記第1の端末装置のネットワークアクセス識別子と上記第1の端末装置に動的に割り当てるアドレスとの対応関係を表すアドレス情報を保持するアドレス情報保持手段と、上記第1の端末装置から上記第2の端末装置へパケットが送出されたときに、上記アドレス情報を保持手段から上記パケットの送信側アドレスに対応するネットワークアクセス識別子を検出し、その検出されたネットワークアクセス識別子に対応するサービス情報を上記サービス情報を保持手段から抽出して有効化する有効化手段と、有効化されたサービス情報に従つてサービスを提供する提供手段と、を有することを特徴とするルータ装置。

【0328】(付記25)第1の端末装置を収容する第1のルータ装置、第2の端末装置を収容する第2のルータ装置、および上記第1および第2の端末装置に提供すべきサービスを規定するサービス情報を管理するサーバ装置を備えるサービス制御ネットワークにおいて、上記第1のルータ装置として使用されるルータ装置であって、上記第1の端末装置に提供すべきサービスを規定す

るサービス情報および上記第2の端末装置に提供すべきサービスを規定するサービス情報を、それぞれ上記第1の端末装置および上記第2の端末装置に設定されているネットワークアクセス識別子と関連づけて保持するサービス情報保持手段と、上記第1の端末装置から上記第2の端末装置へパケットが送出されたときに、上記パケットの受信側アドレスに対応するネットワークアクセス識別子を上記第2のルータ装置から受信し、その受信したネットワークアクセス識別子に対応するサービス情報を上記サービス情報保持手段から抽出して有効化する有効化手段と、有効化されたサービス情報に従ってサービスを提供する提供手段と、を有することを特徴とするルータ装置。

【0329】(付記26) 第1の端末装置を収容する第1のルータ装置、第2の端末装置を収容する第2のルータ装置、および上記第1および第2の端末装置に提供すべきサービスを規定するサービス情報を管理するサーバ装置を備えるサービス制御ネットワークにおいて、上記第1のルータ装置として使用されるルータ装置であって、上記第1の端末装置に提供すべきサービスを規定するサービス情報を上記サーバ装置から受信して保持するサービス情報保持手段と、上記第1の端末装置から上記第2の端末装置へパケットが送出されたときに、上記サービス情報保持手段から上記サービス情報を抽出し、上記第2のルータ装置に使用させるためにその抽出したサービス情報を上記第2のルータ装置へ送出する送出手段と、を有することを特徴とするルータ装置。

【0330】(付記27) モバイルIP v 6端末を収容するルータ装置、上記モバイルIP v 6端末のアドレスを認証するサーバ装置、および上記モバイルIP v 6端末の外部ドメインにおいてその上記モバイルIP v 6端末のアドレスを登録するモビリティアンカーポイントを備え、上記モバイルIP v 6端末に対してサービスを提供するサービス制御ネットワークであって、上記サーバ装置は、上記モバイルIP v 6端末のアドレスを認証する際に、そのモバイルIP v 6端末に提供すべきサービスを規定するサービス情報を上記モビリティアンカーポイントへ配布する配布手段を有し、上記ルータ装置は、上記モバイルIP v 6端末からパケットが送出されたときに、上記モビリティアンカーポイントに対して上記サービス情報を要求する要求手段と、受信したサービス情報に従ってサービスを提供する提供手段とを有し、上記モビリティアンカーポイントは、上記ルータ装置からの要求に応じて上記サービス情報をそのルータ装置へ送出する送出手段を有することを特徴とするサービス制御ネットワーク。

【0331】(付記28) モバイルIP v 6端末を収容するルータ装置、上記モバイルIP v 6端末のアドレスを認証するサーバ装置、および上記モバイルIP v 6端末の外部ドメインにおいてその上記モバイルIP v 6端

末のアドレスを登録するモビリティアンカーポイントを備え、上記モバイルIP v 6端末に対してサービスを提供するサービス制御ネットワークであって、上記モビリティアンカーポイントは、上記モバイルIP v 6端末のアドレス登録に際して、上記サーバ装置に対してそのモバイルIP v 6端末に提供すべきサービスを規定するサービス情報を要求する第1の要求手段と、上記ルータ装置からの要求に応じて、上記サーバ装置から受信したサービス情報をそのルータ装置へ送出する送出手段とを有し、上記サーバ装置は、上記モビリティアンカーポイントからの要求に応じて、上記サービス情報を上記モビリティアンカーポイントへ配布する配布手段を有し、上記ルータ装置は、上記モバイルIP v 6端末からパケットが送出されたときに、上記モビリティアンカーポイントに対して上記サービス情報を要求する第2の要求手段と、上記モビリティアンカーポイントから受信したサービス情報に従ってサービスを提供する提供手段とを有することを特徴とするサービス制御ネットワーク。

【0332】(付記29) モバイルIP v 6端末を収容するルータ装置、上記モバイルIP v 6端末のアドレスを認証するサーバ装置、および上記モバイルIP v 6端末の外部ドメインにおいてその上記モバイルIP v 6端末のアドレスを登録するモビリティアンカーポイントを備え、上記モバイльIP v 6端末に対してサービスを提供するサービス制御ネットワークであって、上記ルータ装置は、上記モバイルIP v 6端末に提供すべきサービスを規定するサービス情報を上記サーバ装置から受信して保持する保持手段と、上記モバイルIP v 6端末のアドレス登録に際して、上記サービス情報を上記モビリティアンカーポイントへ送出する送出手段とを有することを特徴とするサービス制御ネットワーク。

【0333】(付記30) モバイルIP v 6端末を収容するルータ装置、上記モバイルIP v 6端末のアドレスを認証するサーバ装置、および上記モバイルIP v 6端末のアドレスを登録するホームエージェントを備え、上記モバイルIP v 6端末に対してサービスを提供するサービス制御ネットワークであって、上記サーバ装置は、上記モバイルIP v 6端末のアドレスを認証する際に、そのモバイルIP v 6端末に提供すべきサービスを規定するサービス情報を上記ホームエージェントへ配布する配布手段を有し、上記ルータ装置は、上記モバイルIP v 6端末からパケットが送出されたときに、上記ホームエージェントに対して上記サービス情報を要求する要求手段と、受信したサービス情報に従ってサービスを提供する提供手段とを有し、上記ホームエージェントは、上記ルータ装置からの要求に応じて上記サービス情報をそのルータ装置へ送出する送出手段を有することを特徴とするサービス制御ネットワーク。

【0334】(付記31) 端末装置を収容するルータ装置および上記端末装置を認証するサーバ装置を備え、上

記端末装置にサービスを提供するサービス制御ネットワークであって、上記サーバ装置は、提供すべきサービスの送信側アドレスまたは受信側アドレスの少なくとも一方の一部がワイルドカードを用いて指定されているサービス情報を格納する格納手段と、上記ルータ装置からの要求に応じて、対応するサービス情報を配布する配布手段とを有し、上記ルータ装置は、配布されたサービス情報に従ってサービスを提供する提供手段を有することを特徴とするサービス制御ネットワーク。

## 【0335】

【発明の効果】本発明によれば、認証プロトコルを利用してサーバ装置からルータ装置へのサービス情報を配布するネットワークにおいて、アドレス要求手順と認証プロトコルとを連携させたので、アドレスが割り当てられる全ての端末装置についてサービス情報の配布が可能となり、それら各端末装置にそれぞれ対応するサービスを提供できる。

【0336】端末装置に動的にアドレスが割り当てられるネットワークにおいて、通信相手のアドレスが変わった場合であっても、サーバ装置からルータ装置へサービス情報の再配布をする必要がない。このため、ネットワークおよび各通信装置の負荷が軽くなる。

【0337】送信側端末を収容するルータ装置と受信側端末を収容するルータ装置との間でそれらの端末間の通信に係わるサービス情報を授受できるので、サーバ装置にアクセスすることなく、適切なサービスを提供できる。

## 【図面の簡単な説明】

【図1】本発明の実施形態のサービス制御ネットワークの構成を示す図（その1）である。

【図2】本発明の実施形態のサービス制御ネットワークの構成を示す図（その2）である。

【図3】本発明の実施形態のサービス制御ネットワークの構成を示す図（その3）である。

【図4】本発明の実施形態のサービス制御ネットワークの構成を示す図（その4）である。

【図5】サービス制御情報を配布する際の基本シーケンスを示す図である。

【図6】配布されたサービスプロファイルの管理方法を示す図である。

【図7】エッジノードが通信相手のホストアドレス情報を取得するシーケンスを示す図である。

【図8】本実施形態のサービス制御ネットワークの動作の一例（その1）である。

【図9】本実施形態のサービス制御ネットワークの動作の一例（その2）である。

【図10】本実施形態のサービス制御ネットワークの動作の一例（その3）である。

## 【図11】AAAサーバの機能ブロック図である。

## 【図12】サービスプロファイルデータベースの一例を

示す図である。

【図13】(a) はオリジナルサービスプロファイルキャッシュの実施例、(b) はオリジナルホストアドレスキャッシュの実施例である。

【図14】AAAサーバのプロトコル制御部の動作を示すフローチャート（その1）である。

【図15】AAAサーバのプロトコル制御部の動作を示すフローチャート（その2）である。

【図16】AAAサーバのプロトコル制御部の動作を示すフローチャート（その3）である。

【図17】AAAサーバのサービスデータ管理部の動作を示すフローチャートである。

【図18】モビリティアンカーポイントの役割を説明する図である。

【図19】ホームエージェント、モビリティアンカーポイントの機能ブロック図である。

【図20】ホームエージェントまたはモビリティアンカーポイントのプロトコル制御部の動作を示すフローチャート（その1）である。

【図21】ホームエージェントまたはモビリティアンカーポイントのプロトコル制御部の動作を示すフローチャート（その2）である。

【図22】エッジノード、ゲートウェイエッジノードの機能ブロック図である。

【図23】(a) ～(d) は、サービス実行データを構成する各キャッシュの例である。

【図24】サービス実行データの作成方法を説明する図である。

【図25】送信側アドレスおよび受信側アドレスを個別に管理するアドレスキャッシュおよびポリシーテーブルの例である。

【図26】各サービスに対応する送信側アドレスおよび受信側アドレスの組合せを管理する構成のアドレスキャッシュおよびポリシーテーブルの例である。

【図27】エッジノードまたはゲートウェイエッジノードのサービス制御部の動作を示すフローチャートである。

【図28】アドレスキャッシュをチェックする処理のフローチャート（その1）である。

【図29】アドレスキャッシュをチェックする処理のフローチャート（その2）である。

【図30】エッジノードまたはゲートウェイエッジノードのパケット編集部の動作を示すフローチャートである。

【図31】エッジノードまたはゲートウェイエッジノードのプロトコル制御部の動作を示すフローチャート（その1）である。

【図32】エッジノードまたはゲートウェイエッジノードのプロトコル制御部の動作を示すフローチャート（その2）である。

【図33】エッジノードまたはゲートウェイエッジノードのプロトコル制御部の動作を示すフローチャート（その3）である。

【図34】エッジノードまたはゲートウェイエッジノードのプロトコル制御部の動作を示すフローチャート（その4）である。

【図35】エッジノードまたはゲートウェイエッジノードのサービスデータ管理部の動作を示すフローチャートである。

【図36】アドレスキャッシュにおいてヒットミスが発生した場合の処理のフローチャート（その1）である。

【図37】アドレスキャッシュにおいてヒットミスが発生した場合の処理のフローチャート（その2）である。

【図38】サービスプロファイルの有効化について説明するためのネットワーク構成の例である。

【図39】サービスプロファイルをマージする処理のフローチャート（その1）である。

【図40】サービスプロファイルをマージする処理のフローチャート（その2）である。

【図41】IP v6アドレスのライフタイムオーバが発生した場合の処理のフローチャート（その1）である。

【図42】IP v6アドレスのライフタイムオーバが発生した場合の処理のフローチャート（その2）である。

【図43】ホームドメイン内のエッジノードにサービス情報を配布するシーケンスを示す図である。

【図44】外部ドメインのエッジノードにサービス情報を配布するシーケンスを示す図である。

【図45】ゲートウェイエッジノードにサービス情報を配布するシーケンスを示す図である。

【図46】ホームエージェントにサービス情報を配布するシーケンスを示す図である。

【図47】モビリティアンカーポイントにサービス情報を配布するシーケンス（その1）を示す図である。

【図48】モビリティアンカーポイントにサービス情報を配布するシーケンス（その2）を示す図である。

【図49】モビリティアンカーポイントにサービス情報を配布するシーケンス（その3）を示す図である。

【図50】送信側エッジノードが受信側エッジノードから制御情報を取得するシーケンスを示す図である。

【図51】送信側エッジノードから受信側エッジノードへ制御情報を送るシーケンスを示す図である。

【図52】送信側エッジノードおよび受信側エッジノードが相互に制御情報を送るシーケンスを示す図である。

【図53】エッジノードがホームエージェントから制御情報を取得するシーケンスを示す図である。

【図54】エッジノードがモビリティアンカーポイントから制御情報を取得するシーケンスを示す図である。

【図55】送信側ヒットミスが発生した際の有効化処理のシーケンスを示す図である。

【図56】受信側ヒットミスが発生した際の有効化処理

50

のシーケンスを示す図である。

【図57】送信側ヒットミスおよび受信側ヒットミスが発生した際の有効化処理のシーケンスを示す図である。

【図58】送信側アドレスおよび受信側アドレスの組合せが登録されている場合の有効化処理のシーケンスである。

【図59】送信側アドレスのライフタイムが消滅した場合の無効化処理のシーケンスを示す図である。

【図60】受信側アドレスのライフタイムが消滅した場合の無効化処理のシーケンスを示す図である。

【図61】送信側アドレスおよび受信側アドレスの組合せが登録されている場合の無効化処理のシーケンスである。

【図62】IP v6ホストからの要求によりサービスを無効化するシーケンスを示す図である。

【図63】IP v6ホストからの要求により他のノードのサービス情報を削除／無効化するシーケンスを示す図である。

【図64】IP v6ヘッダの構成を示す図である。

【図65】ICMP-A AA要求メッセージの構成を示す図である。

【図66】ICMP-A AA応答メッセージの構成を示す図である。

【図67】D I A M E T E Rメッセージを伝送するパケットの構成を示す図である。

【図68】(a) および(b) は、それぞれ、A H R (A M R) メッセージおよびA H A (A M A) メッセージのデータ構成を示す図である。

【図69】(a) および(b) は、それぞれ、A S R メッセージおよびA S A メッセージのデータ構成を示す図である。

【図70】(a) ～(d) は、それぞれH H R メッセージ、H H A メッセージ、S T R メッセージ、S T A メッセージのデータ構成を示す図である。

【図71】N A I - S P C要求メッセージのデータ構成を説明する図である。

【図72】N A I - S P C応答メッセージのデータ構成を説明する図である。

【図73】結合更新メッセージのデータ構成を説明する図である。

【図74】I C M P - A A A - T e a r d o w n要求メッセージのデータ構成を説明する図である。

【図75】I C M P - A A A - T e a r d o w n応答メッセージのデータ構成を説明する図である。

【符号の説明】

1 A A A サーバ (A A A H)

2 A A A サーバ (A A A L)

1 1, 1 2 I P v6 ホスト

2 1, 2 2 エッジノード

3 1, 3 2 ゲートウェイエッジノード

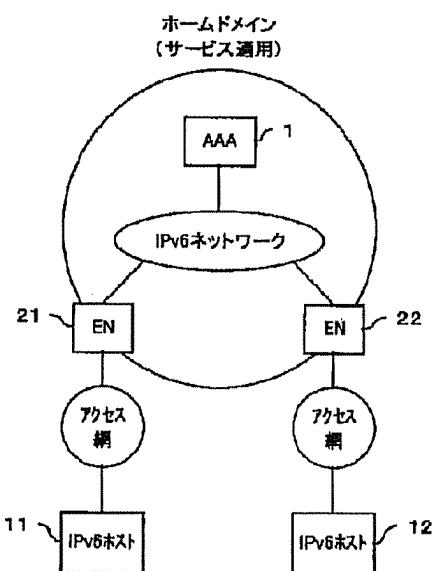
73

74

4 1	移動ノード	1 0 4	サービスプロファイルデータベース
4 2	通信ノード	1 0 5、 2 0 4、 3 0 6	サービス規定データ
4 3	ホームエージェント	3 0 2	サービス制御部
4 4、 4 5	モビリティアンカーポイント	3 0 3	パケット編集部
5 1	データベース	3 0 7	サービス実行データ
1 0 2、 2 0 2、 3 0 4	プロトコル制御部	3 0 8	サービス制御データ
1 0 3、 2 0 3、 3 0 5	サービスデータ制御部		

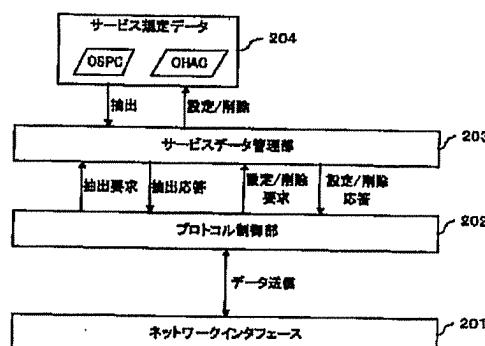
【図1】

本発明の実施形態のサービス制御ネットワークの構成を示す図(その1)



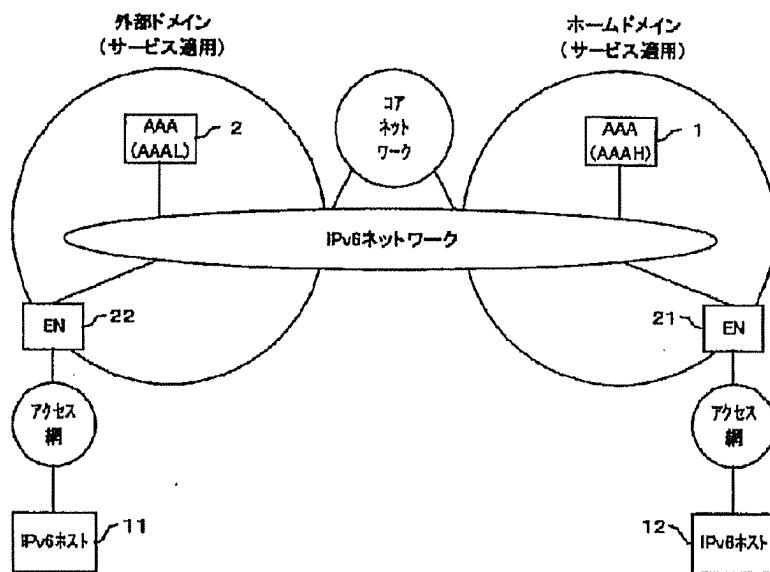
【図19】

ホームエージェント、モビリティアンカーポイントの機能ブロック図

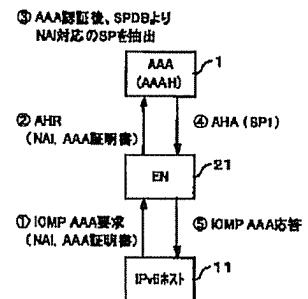


【図2】

本発明の実施形態のサービス制御ネットワークの構成を示す図(その2)



【図43】

ホームドメイン内のエッジノードに  
サービス情報を配布するシーケンスを示す図

【図12】

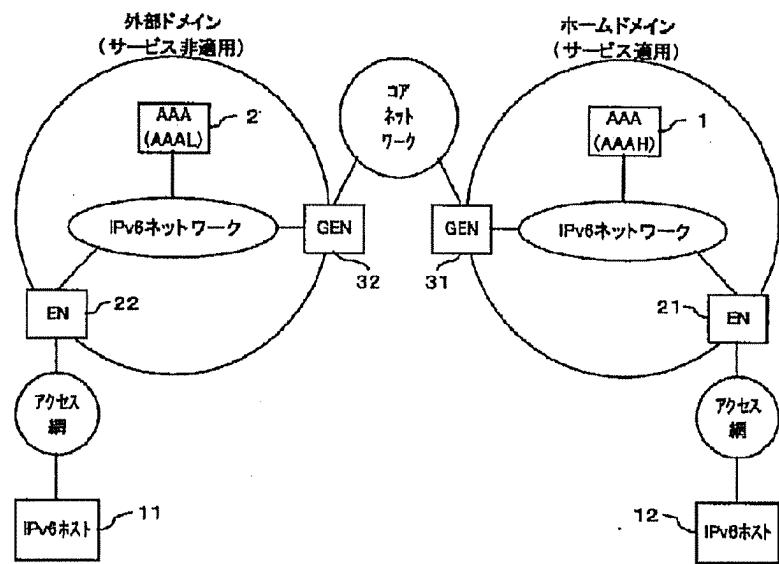
サービスプロファイルデータベースの一例を示す図

サービスプロファイルデータベース (SPDB)

構成要素	説明
SrcNAI	送信側 NAI
SrcAddr	送信側 IPv6 アドレス
SrcNetmask	送信側 ネットマスク
SrcPort	送信側 ポート番号
DstNAI	受信側 NAI
DstAddr	受信側 IPv6 アドレス
DstNetmask	受信側 ネットマスク
DstPort	受信側 ポート番号
SIInf	サービス情報 (QoS 等)

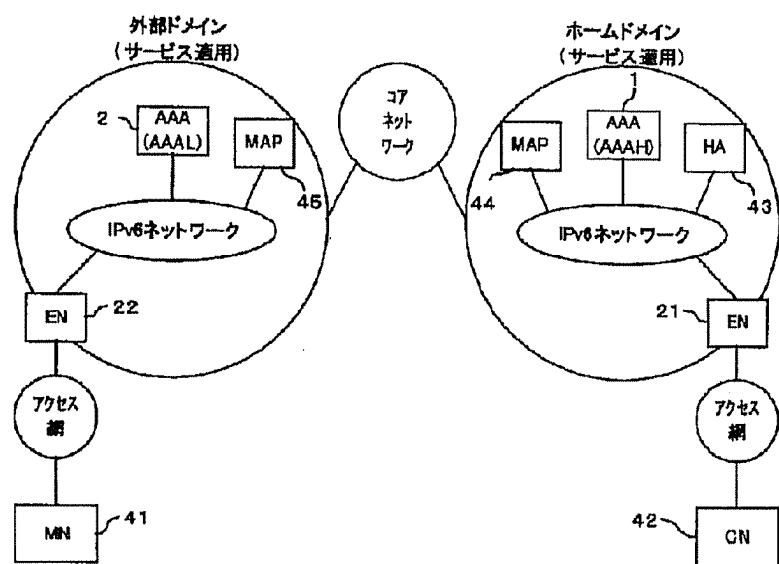
【図3】

本発明の実施形態のサービス制御ネットワークの構成を示す図(その3)



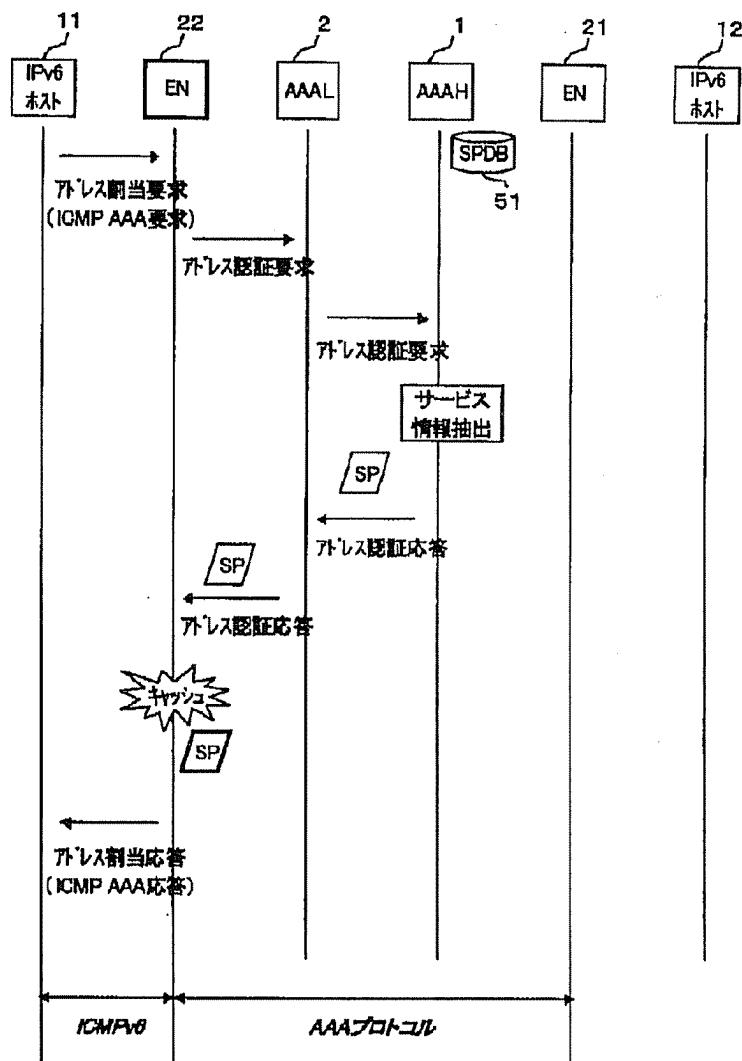
【図4】

本発明の実施形態のサービス制御ネットワークの構成を示す図(その4)



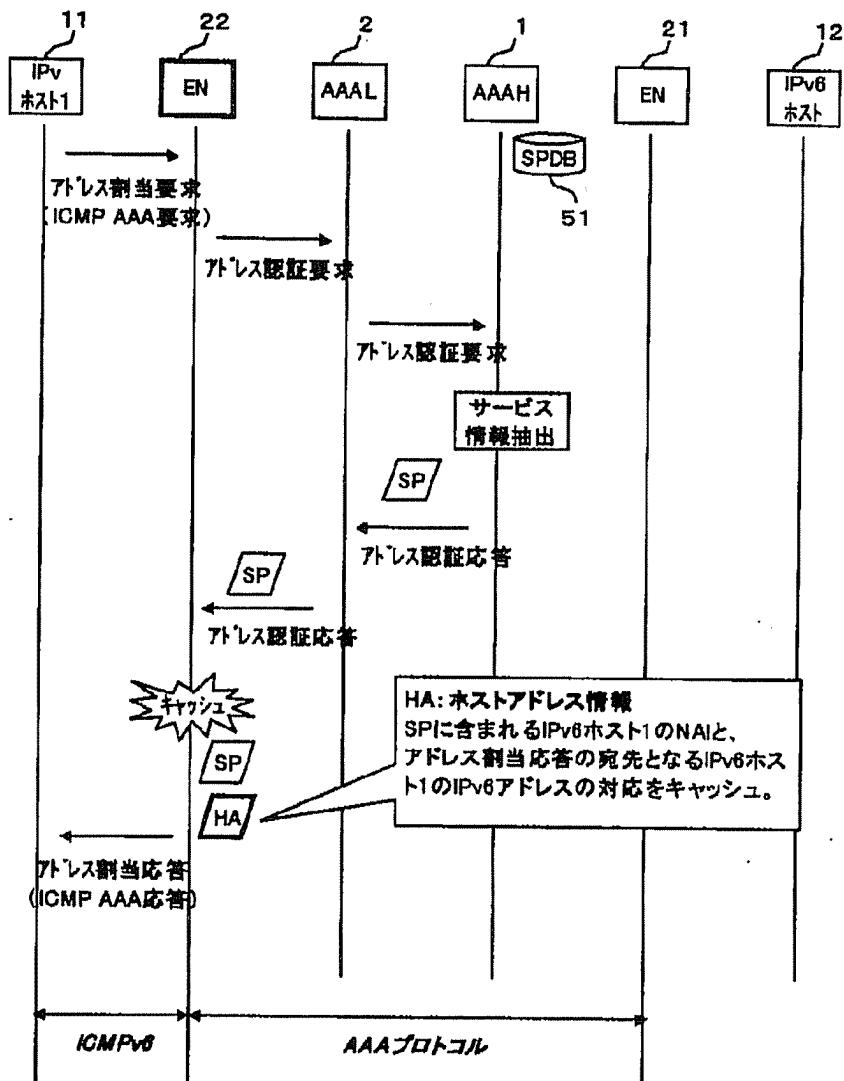
【図5】

## サービス制御情報を配布する際の基本シーケンスを示す図



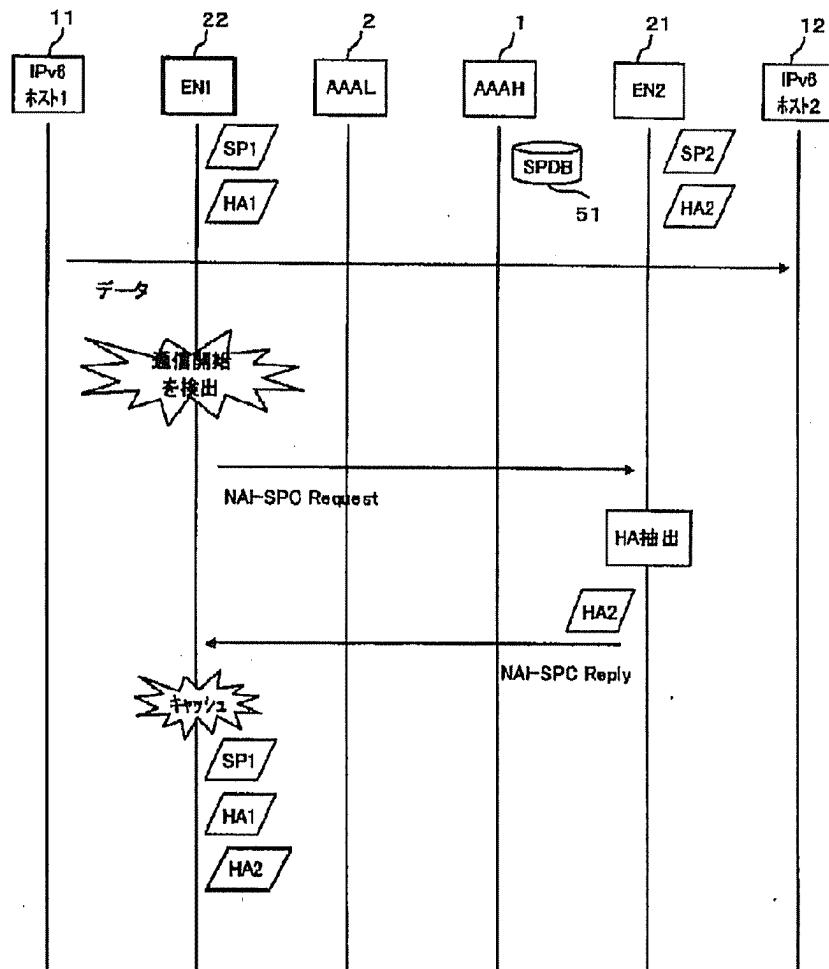
【図6】

## 配布されたサービスプロファイルの管理方法を示す図



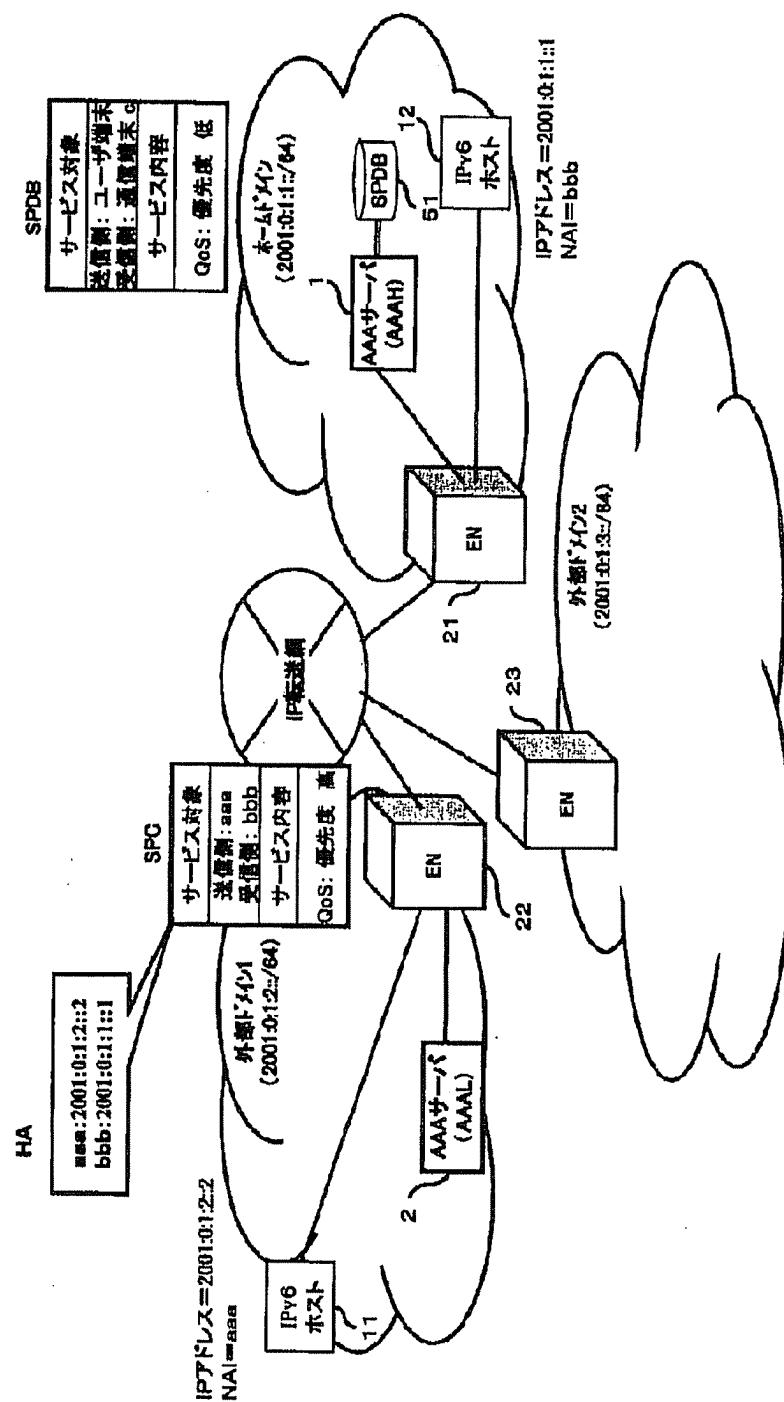
【図7】

エッジノードが通信相手のホストアドレス情報を取得する  
シーケンスを示す図



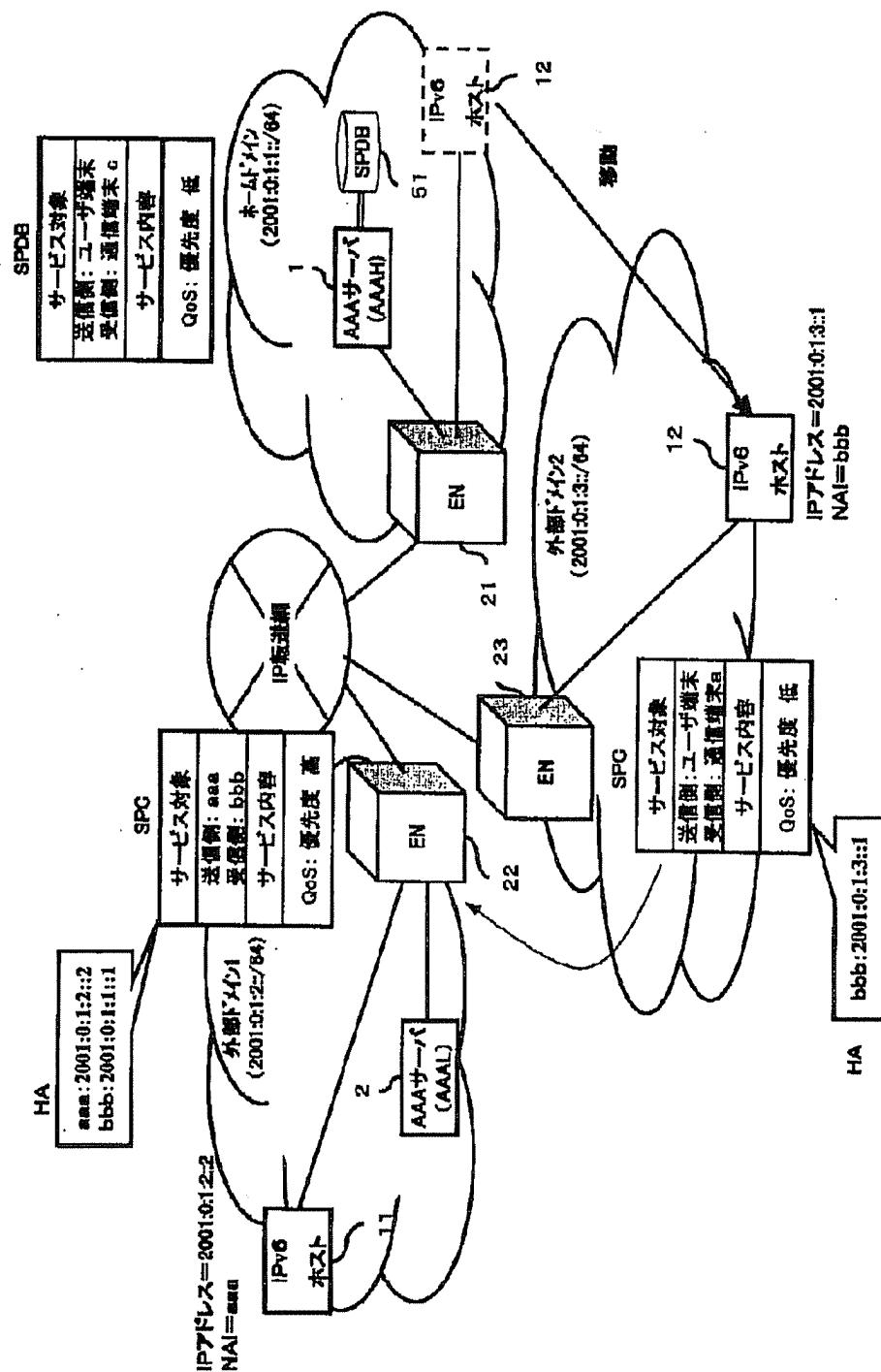
【図8】

## 本実施形態のサービス制御ネットワークの動作の一例(その1)



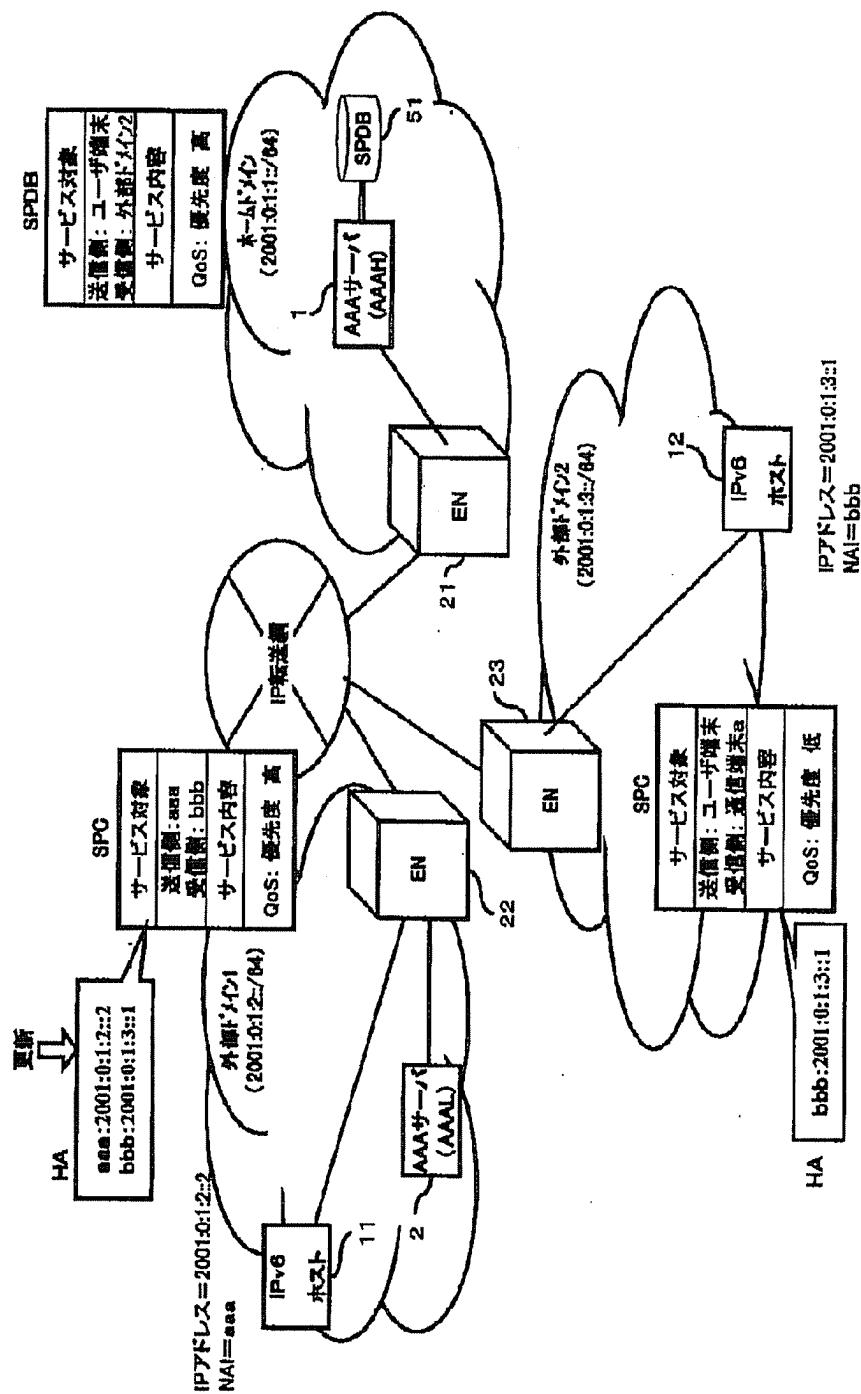
【図9】

## 本実施形態のサービス制御ネットワークの動作の一例(その2)



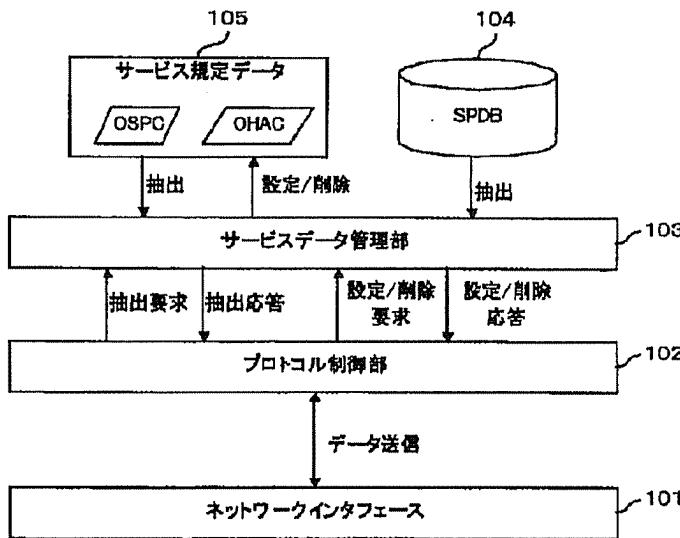
【図10】

## 本実施形態のサービス制御ネットワークの動作の一例(その3)



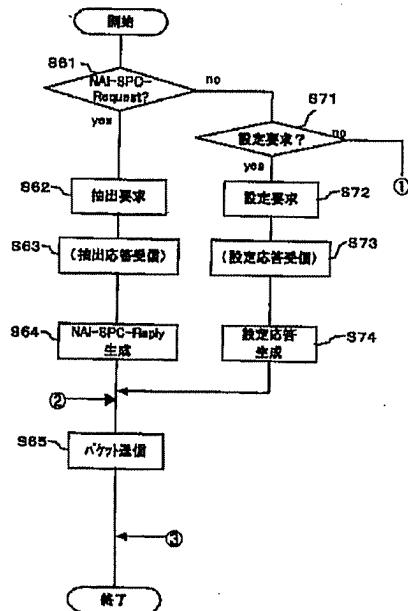
【図11】

## AAAサーバの機能ブロック図



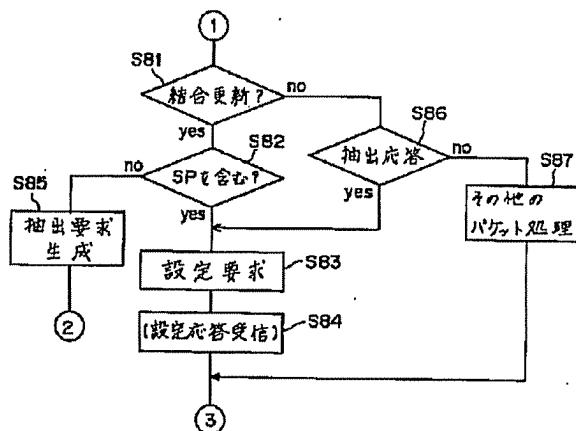
【図20】

## ホームエージェントまたはモビリティアンカーポイントのプロトコル制御部の動作を示すフローチャート(その1)



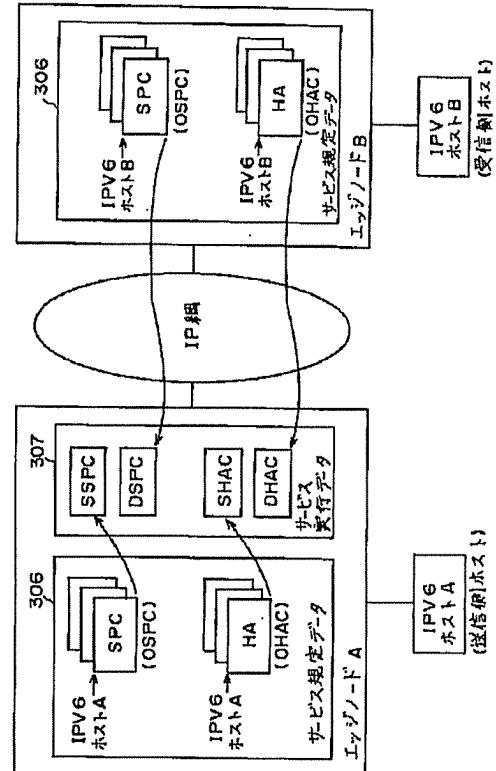
【図21】

## ホームエージェントまたはモビリティアンカーポイントのプロトコル制御部の動作を示すフローチャート(その2)



【図24】

## サービス実行データの作成方法を説明する図



## 【図13】

(a)はオリジナルサービスプロファイルキャッシュの実施例、  
 (b)はオリジナルホストアドレスキャッシュの実施例

オリジナルサービスプロファイルキャッシュ (DSPC)	
構成要素	説明
NAI-ID	管理ホスト NAI識別子
SrcNAI	送信側 NAI
SrcAddr	送信側 IPv6 アドレス
SrcNetmask	送信側ネットマスク
SrcPort	送信側ポート番号
DstNAI	受信側 NAI
DstAddr	受信側 IPv6 アドレス
DstNetmask	受信側ネットマスク
DstPort	受信側ポート番号
Sinf	サービス情報 (QoS 等)

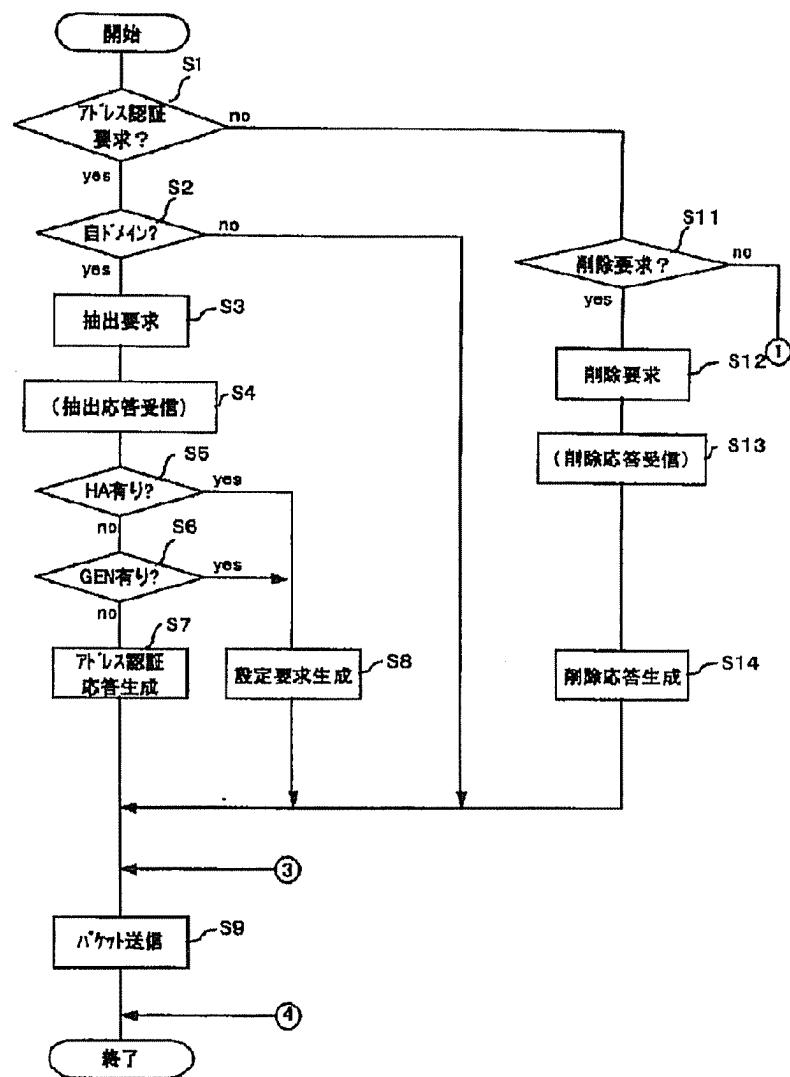
(a)

オリジナルホストアドレスキャッシュ (OHAC)	
構成要素	説明
NAI-ID	管理ホスト NAI 識別子
IPAddr	管理ホスト IPv6 アドレス
Lifetime	有効時間
AAAInf	AAA 関連情報
Export Addr	送出先 IPv6 アドレス

(b)

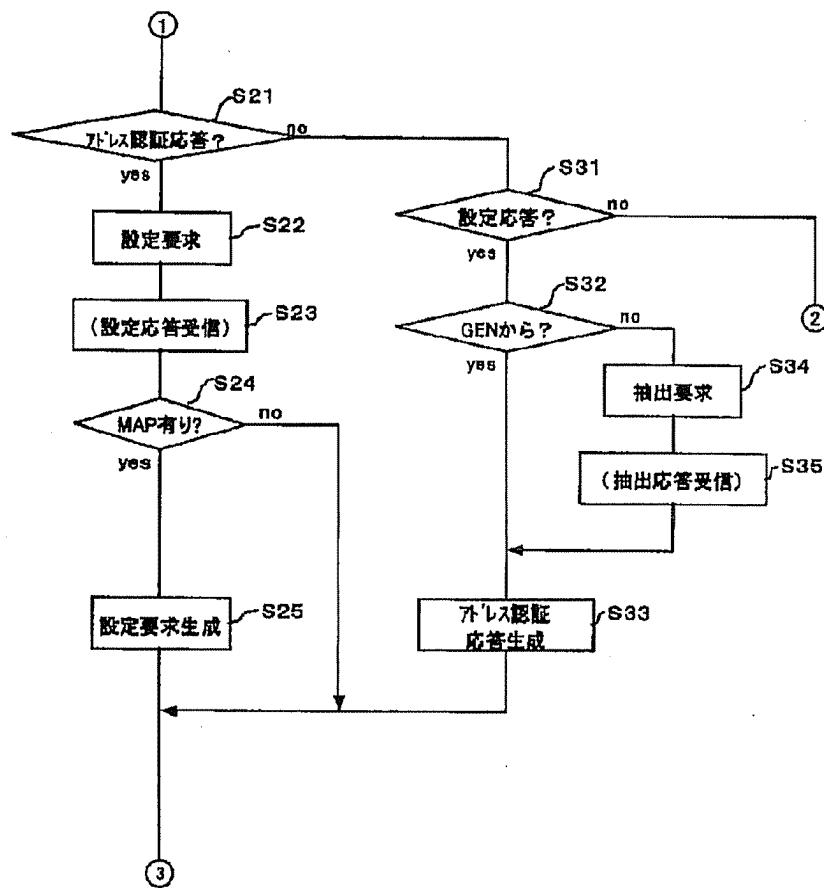
【図14】

## AAAサーバのプロトコル制御部の動作を示すフローチャート(その1)



〔図15〕

## AAAサーバのプロトコル制御部の動作を示すフローチャート(その2)

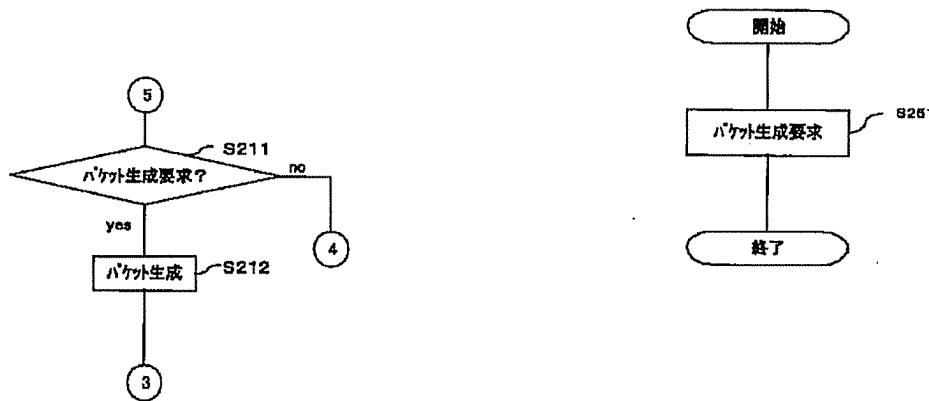


〔四三四〕

## エッジノードまたはゲートウェイエッジノードの プロトコル制御部の動作を示すフローチャート(その4)

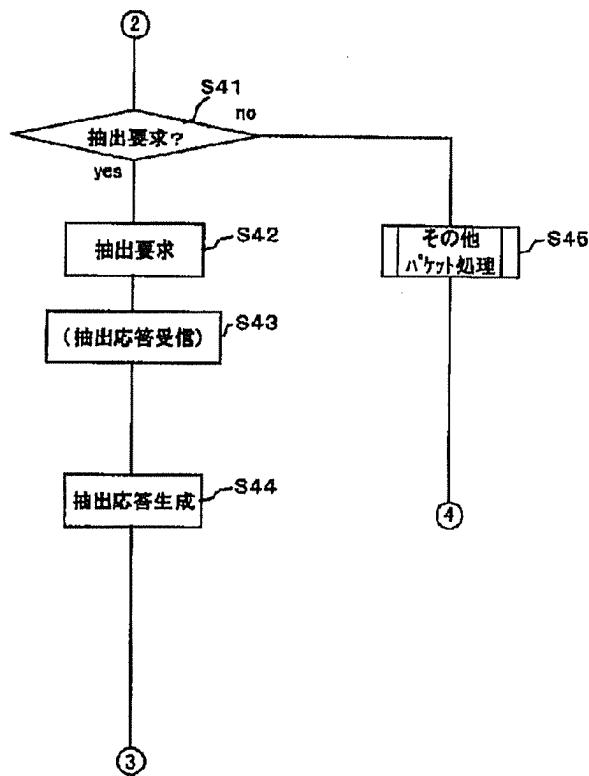
【図37】

## アドレスキャッシュにおいてヒットミスが発生した場合の 処理のフローチャート(その2)



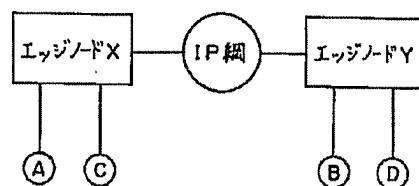
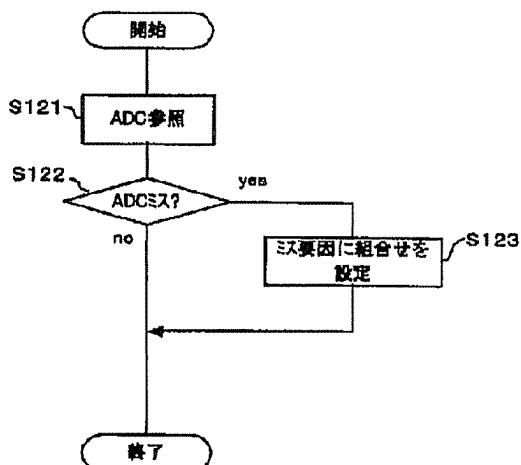
【図16】

AAAサーバのプロトコル制御部の動作を示すフローチャート(その3)



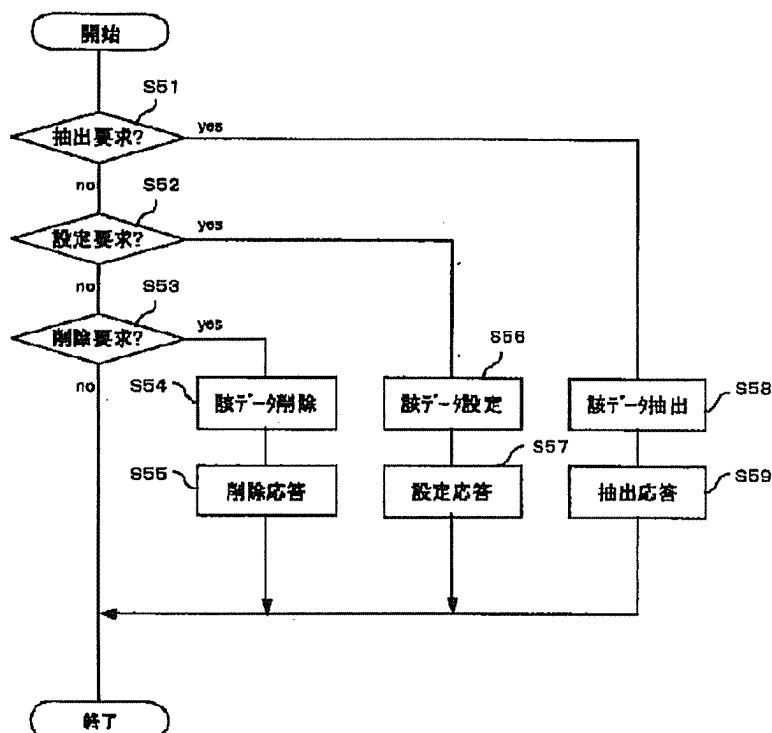
【図29】

【図38】

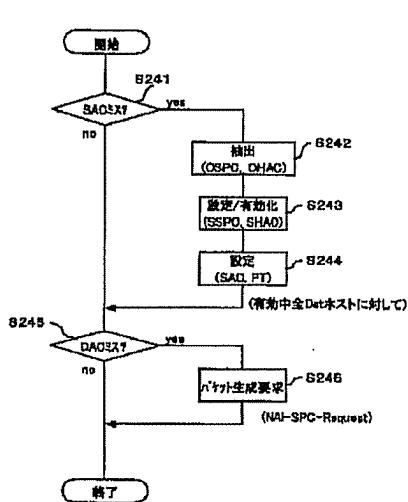
アドレスキャッシュをチェックする処理のフローチャート(その2)  
サービスプロファイルの有効化について  
説明するためのネットワーク構成の例

【図17】

AAAサーバのサービスデータ管理部の動作を示すフローチャート

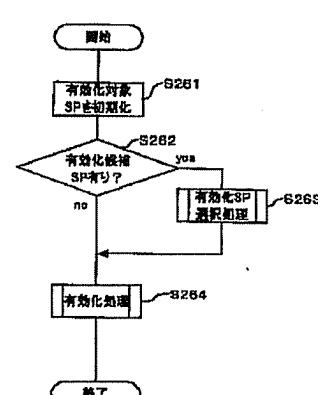


【図36】

アドレスキャッシュにおいてヒットミスが発生した場合の  
処理のフローチャート(その1)

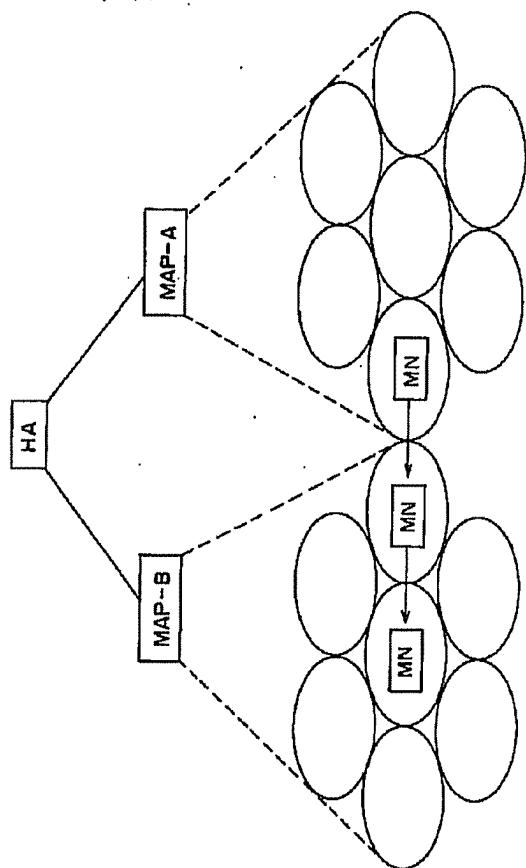
【図39】

サービスプロファイルをマージする処理のフローチャート(その1)



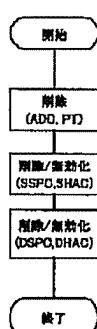
【図18】

モビリティアンカーポイントの役割を説明する図



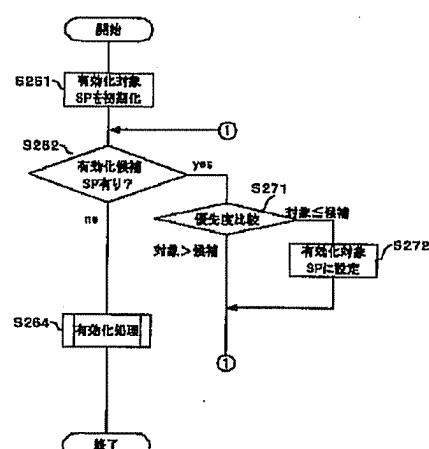
【図42】

IPv6アドレスのライフタイムオーバーが発生した場合の処理のフローチャート(その2)



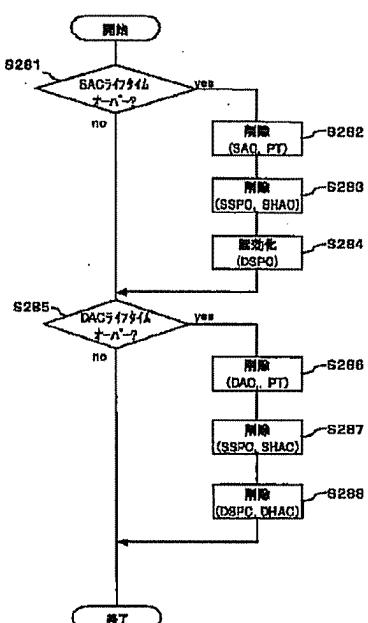
【図40】

サービスプロファイルをマージする処理のフローチャート(その2)



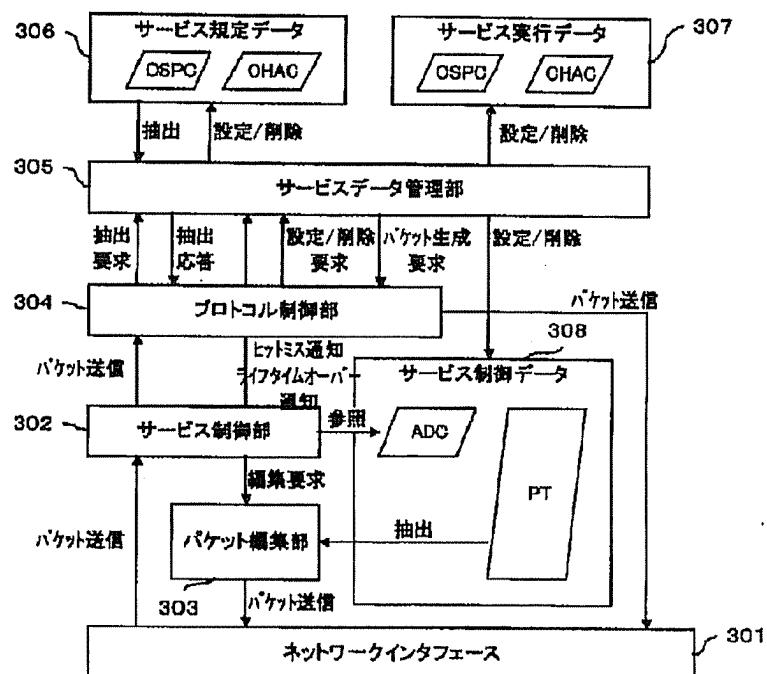
【図41】

IPv6アドレスのライフタイムオーバーが発生した場合の処理のフローチャート(その1)



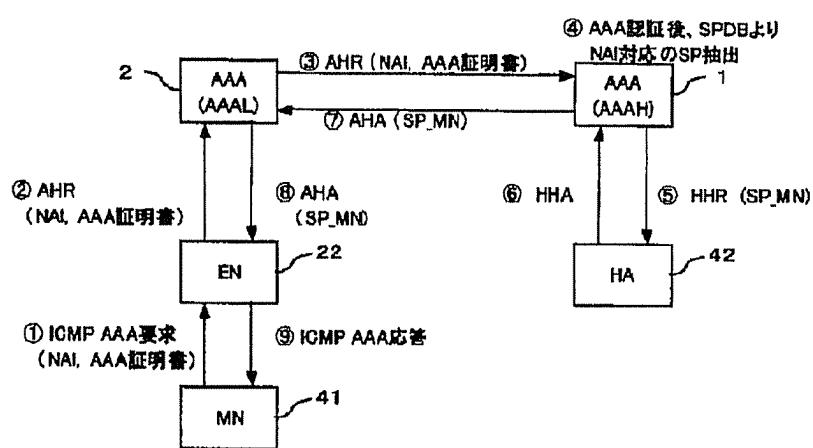
【図22】

## エッジノード、ゲートウェイエッジノードの機能ブロック図



【図46】

## ホームエージェントにサービス情報を配布するシーケンスを示す図



【図23】

(a)～(d)は、サービス実行データを構成する各キャッシュの例

コミュニケーションサービスプロファイルキャッシュ (CSPC)

送信側サービスプロファイルキャッシュ (SSPC)

構成要素		説明
SPC-ID		サービスプロファイル識別子
SrcNAI		送信側 NAI
SrcAddr		送信側 IPv6 アドレス
SrcNetmask		送信側ネットマスク
SrcPort		送信側ポート番号
DstNAI		受信側 NAI
DstAddr		受信側 IPv6 アドレス
DstNetmask		受信側ネットマスク
DstPort		受信側ポート番号
Sinf		サービス情報 (QoS 等)
State		サービス実行状態 (有効/無効)

受信側サービスプロファイルキャッシュ (DSPC)

構成要素		説明
SPC-ID		サービスプロファイル識別子
SrcNAI		送信側 NAI
SrcAddr		送信側 IPv6 アドレス
SrcNetmask		送信側ネットマスク
SrcPort		送信側ポート番号
DstNAI		受信側 NAI
DstAddr		受信側 IPv6 アドレス
DstNetmask		受信側ネットマスク
DstPort		受信側ポート番号
Sinf		サービス情報 (QoS 等)
State		サービス実行状態 (有効/無効)

コミュニケーションホストアドレスキャッシュ (CHAC)

送信側ホストアドレスキャッシュ (SHAC)

構成要素		説明
SrcNAI		送信側ホスト NAI
SrcAddr		送信側 IPv6 アドレス

受信側ホストアドレスキャッシュ (DHAC)

構成要素		説明
DstNAI		受信側ホスト NAI
DstAddr		受信側 IPv6 アドレス

【图25】

送信側アドレスおよび受信側アドレスを個別に管理する  
アドレスキャッシュおよびポリシーテーブルの例

### アドレスキャッシュ (ADC)

### 送信側アドレスキャッシュ (SAC)

構成要素		説明
SrcAddr	送信側 IPv6 アドレス	
Lifetime	送信側アドレスキャッシュ有効時間	

### 受信側アドレスキャッシュ (DCC)

構成要素		説明
DstAddr	受信側 IPv6 アドレス	
Lifetime	受信側アドレスキャッシュ有効時間	

### ポリシーテープル (PT)

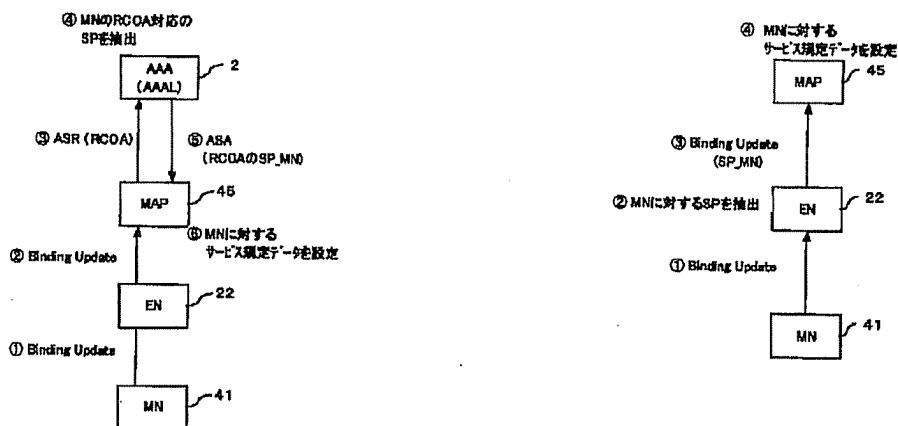
構成要素	説明
SrcAddr	送信側 IPv6 アドレス
SrcNetmask	送信側ネットマスク
SrcPort	送信側ポート番号
DstAddr	受信側 IPv6 アドレス
DstNetmask	受信側ネットマスク
DstPort	受信側ポート番号
Smf	サービス情報 (QoS 等)

[图48]

【図49】

## モビリティアンカーポイントにサービス情報を配布する シーケンス(その2)を示す図

### モビリティアンカーポイントにサービス情報を配布する シーケンス(その3)を示す図



【図26】

各サービスに対応する送信側アドレスおよび受信側アドレスの組合せを管理する構成のアドレスキャッシュおよびポリシーテーブルの例

アドレスキャッシュ(ADC)

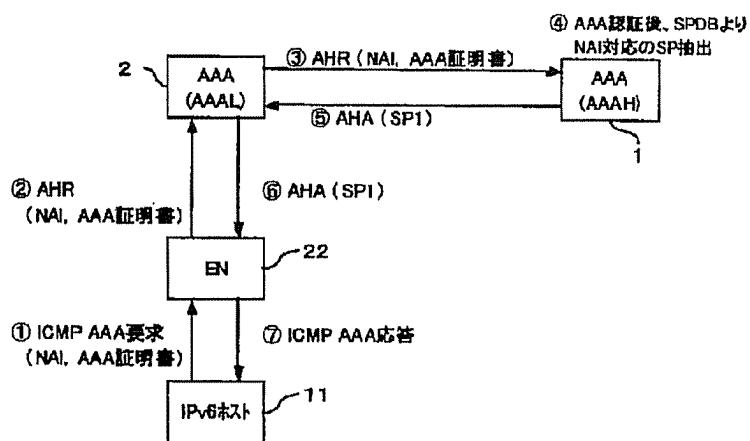
構成要素	説明
SrcAddr	送信側 IPv6 アドレス
DstAddr	受信側 IPv6 アドレス
Lifetime	アドレスキャッシュ有効時間

ポリシーテーブル(PT)

構成要素	説明
SPC-ID	サービスプロファイル識別子
SrcAddr	送信側 IPv6 アドレス
SrcNetmask	送信側ネットマスク
SrcPort	送信側ポート番号
DstAddr	受信側 IPv6 アドレス
DstNetmask	受信側ネットマスク
DstPort	受信側ポート番号
Sinf	サービス情報 (QoS 等)

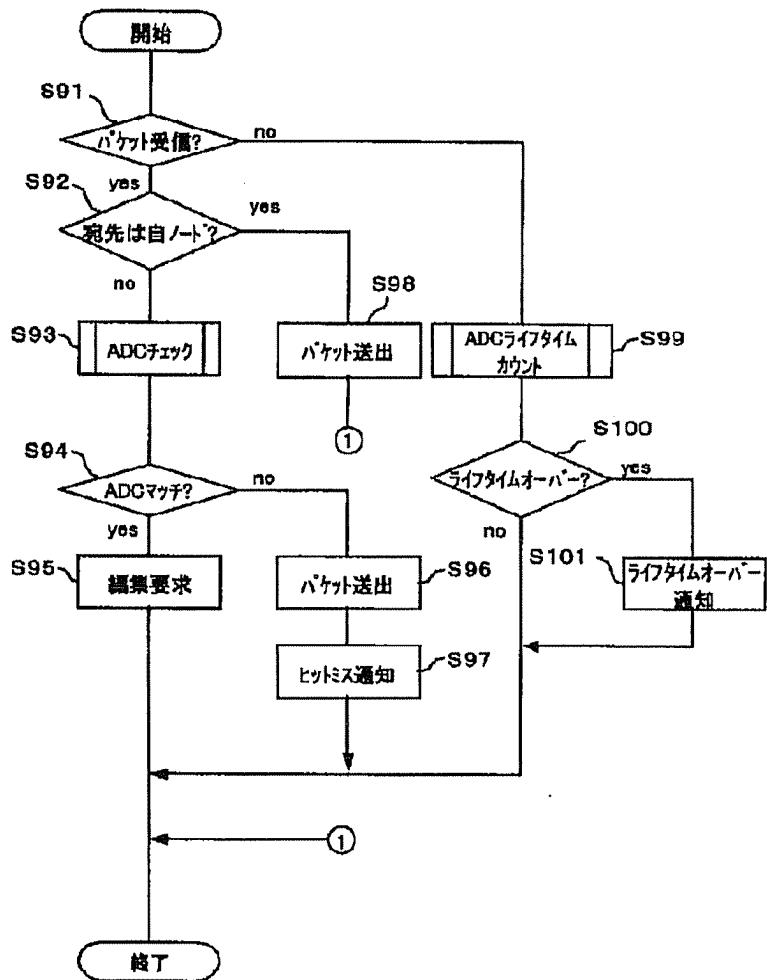
【図44】

外部ドメインのエッジノードにサービス情報を配布するシーケンスを示す図



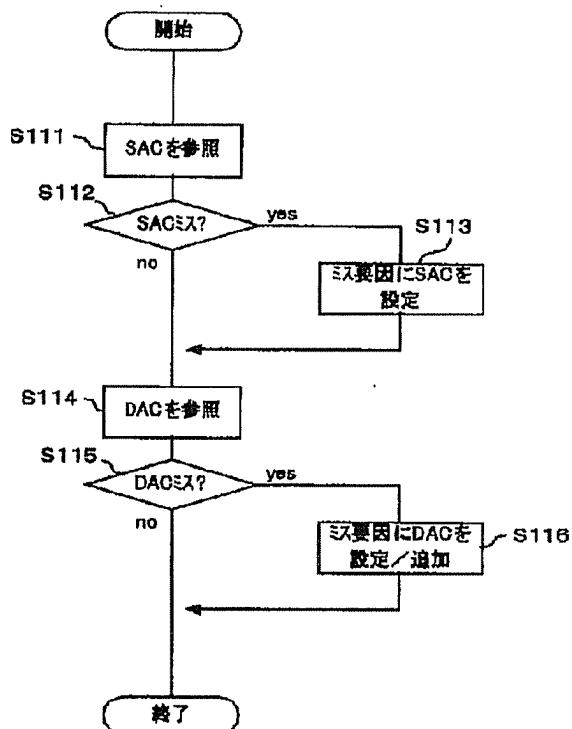
【図27】

エッジノードまたはゲートウェイエッジノードの  
サービス制御部の動作を示すフロー・チャート



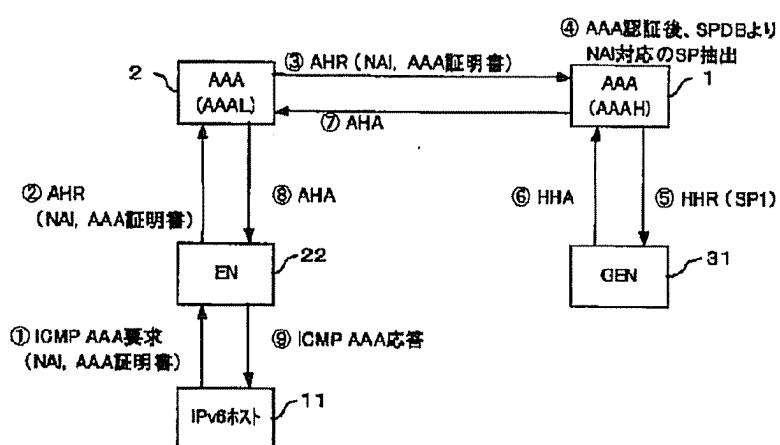
【図28】

## アドレスキャッシュをチェックする処理のフローチャート(その1)



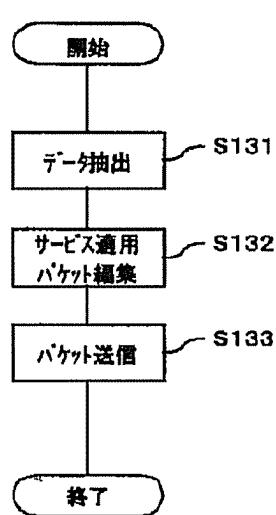
【図45】

## ゲートウェイエッジノードにサービス情報を配布するシーケンスを示す図



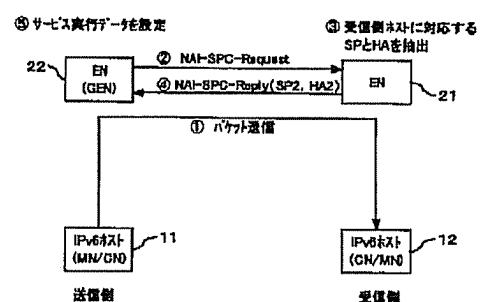
【図30】

エッジノードまたはゲートウェイエッジノードの  
パケット編集部の動作を示すフローチャート



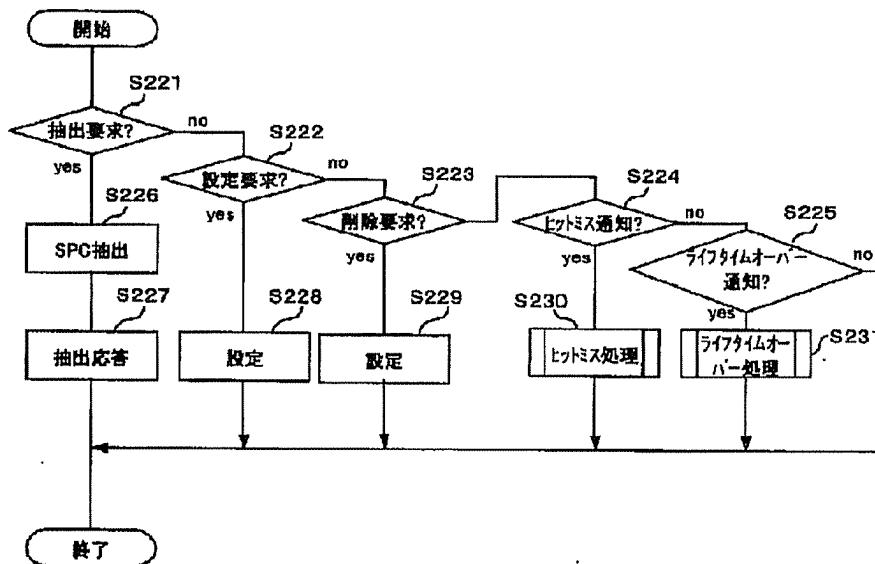
【図50】

送信側エッジノードが受信側エッジノードから  
制御情報を取得するシーケンスを示す図



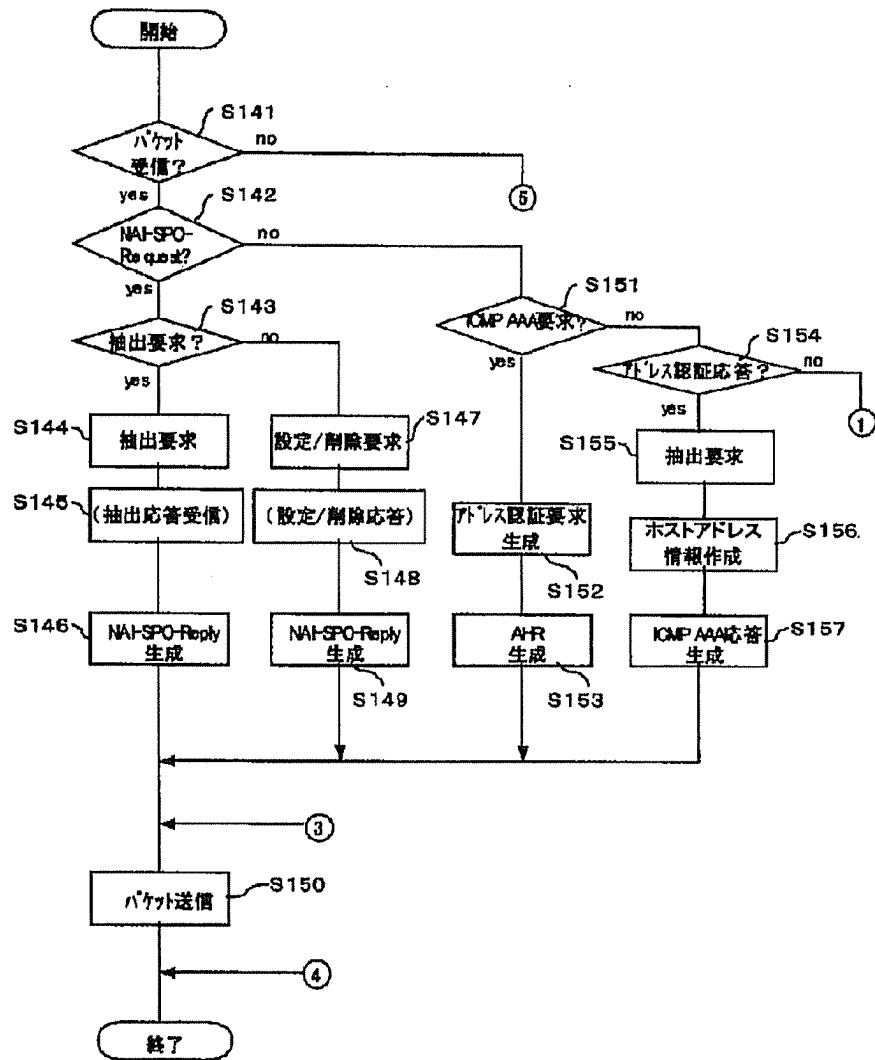
【図35】

エッジノードまたはゲートウェイエッジノードの  
サービスデータ管理部の動作を示すフローチャート



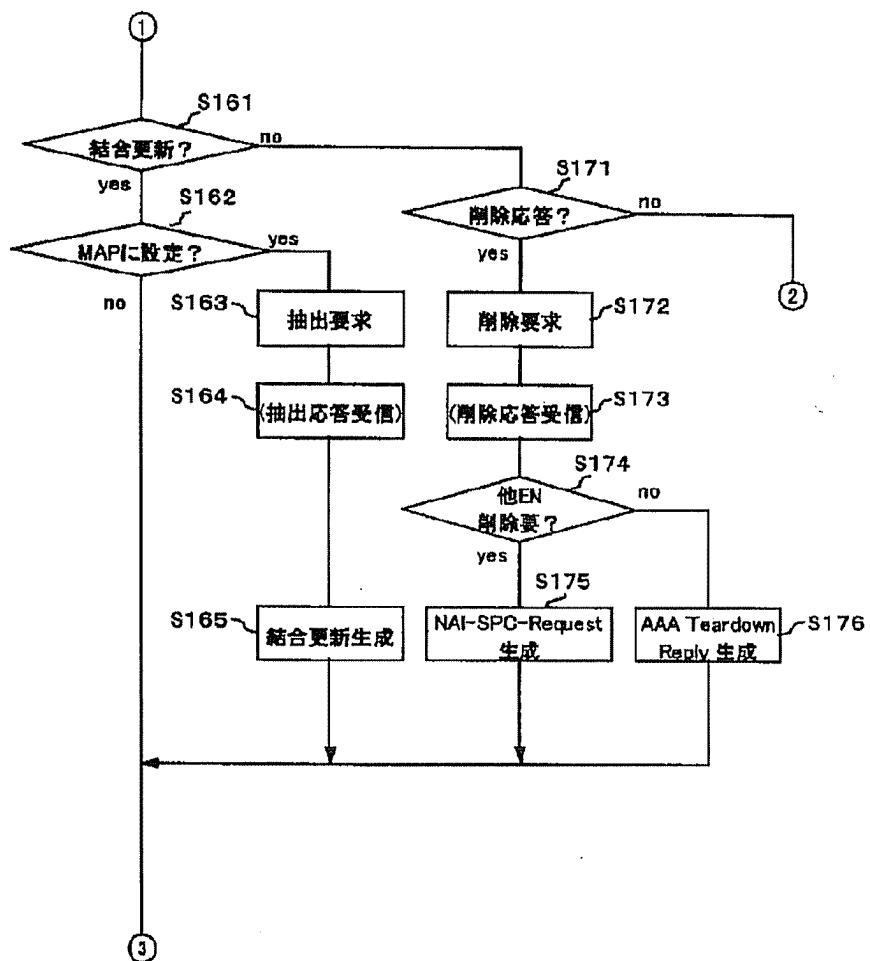
【図31】

## エッジノードまたはゲートウェイエッジノードの プロトコル制御部の動作を示すフローチャート(その1)



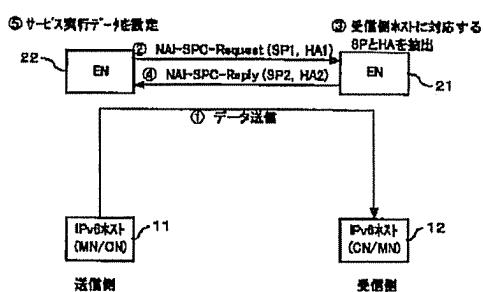
【図32】

エッジノードまたはゲートウェイエッジノードの  
プロトコル制御部の動作を示すフローチャート(その2)



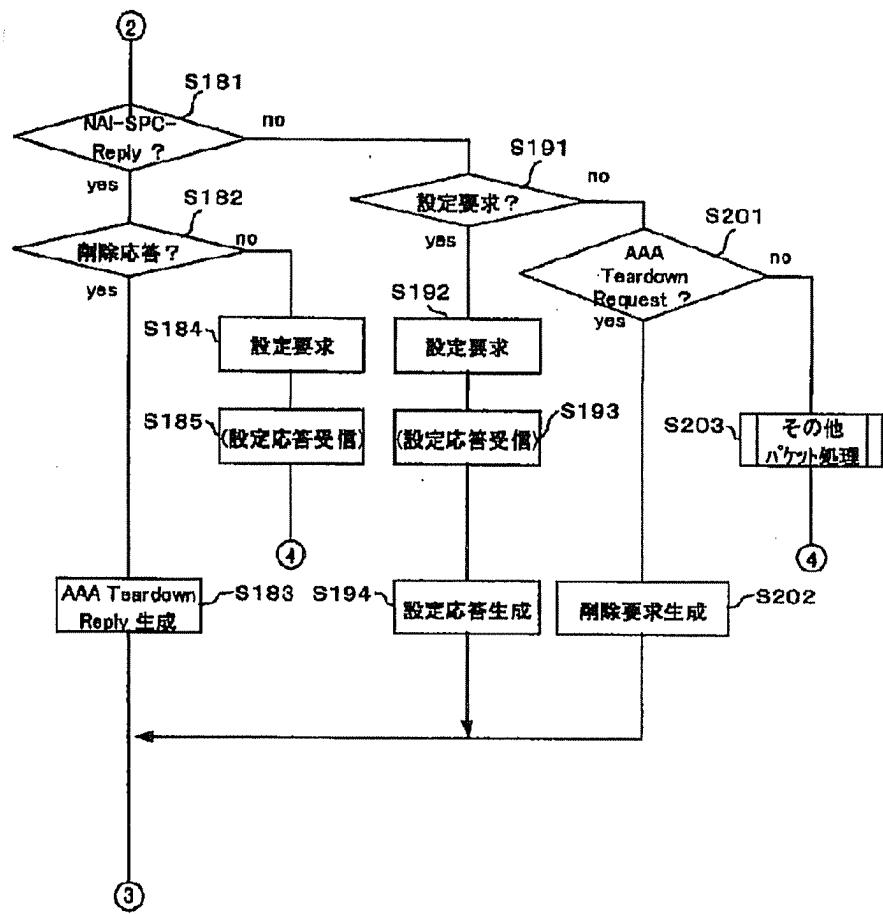
【図52】

送信側エッジノードおよび受信側エッジノードが相互に  
制御情報を送るシーケンスを示す図



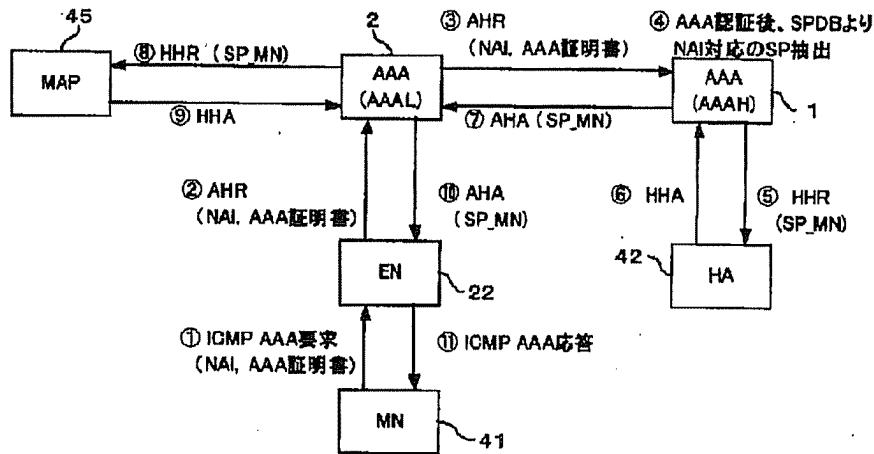
【四三三】

### エッジノードまたはゲートウェイエッジノードの プロトコル制御部の動作を示すフローチャート(その3)



【図47】

モビリティアンカーポイントにサービス情報を配布する  
シーケンス(その1)を示す図

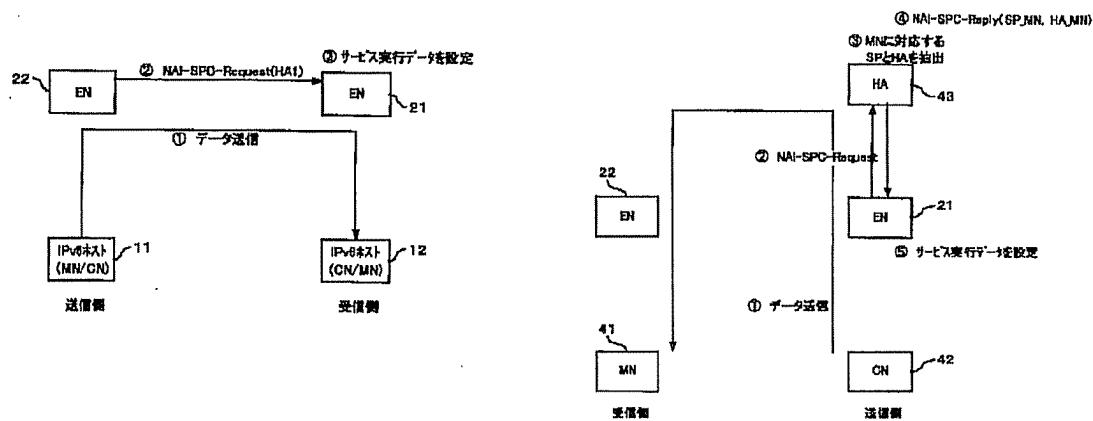


【図51】

送信側エッジノードから受信側エッジノードへ  
制御情報を送るシーケンスを示す図

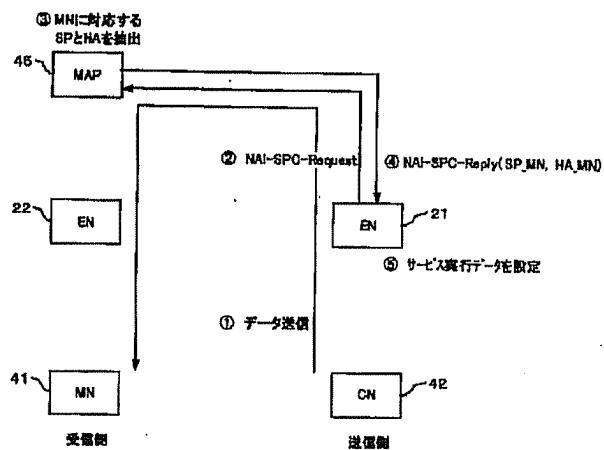
【図53】

エッジノードがホームエージェントから制御情報を取得する  
シーケンスを示す図



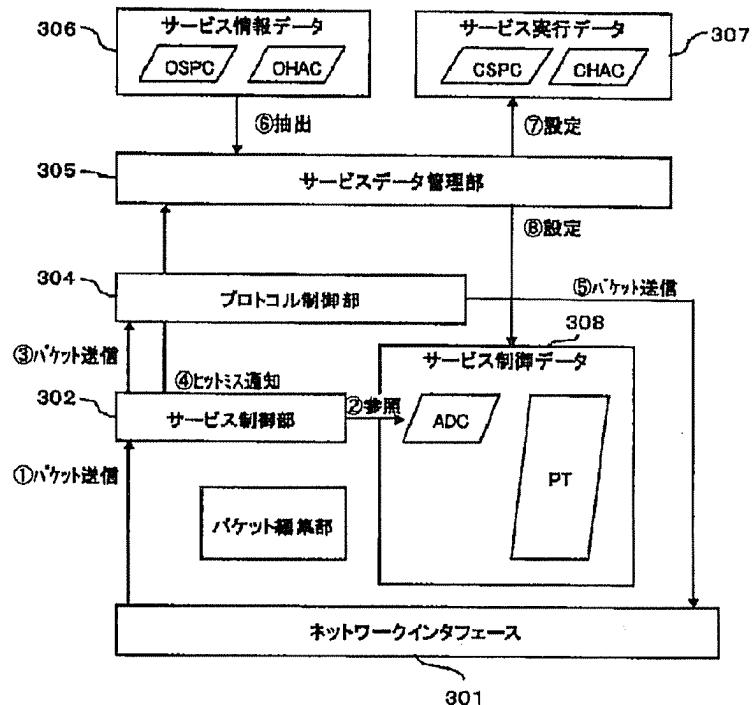
【図54】

エッジノードがモビリティアンカーポイントから  
制御情報を取得するシーケンスを示す図



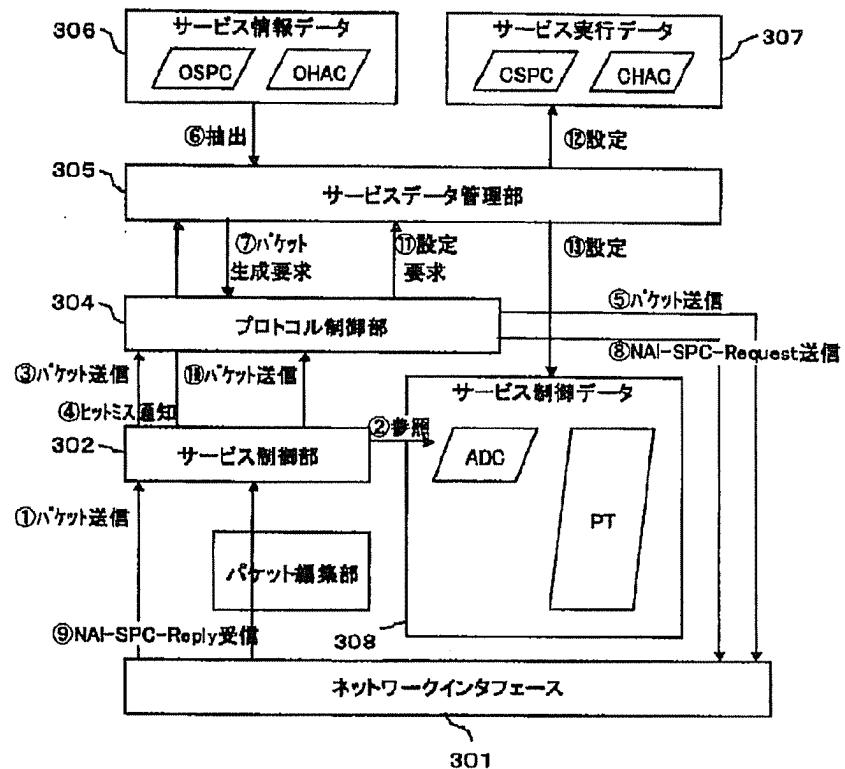
【図55】

送信側ヒットミスが発生した際の  
有効化処理のシーケンスを示す図



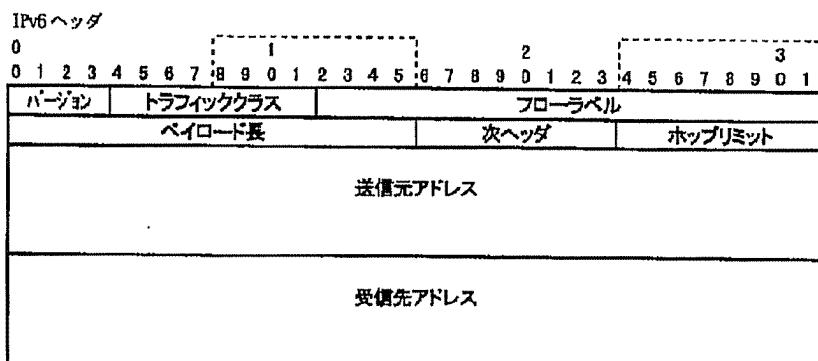
【図 5 6】

受信側ヒットミスが発生した際の  
有効化処理のシーケンスを示す図



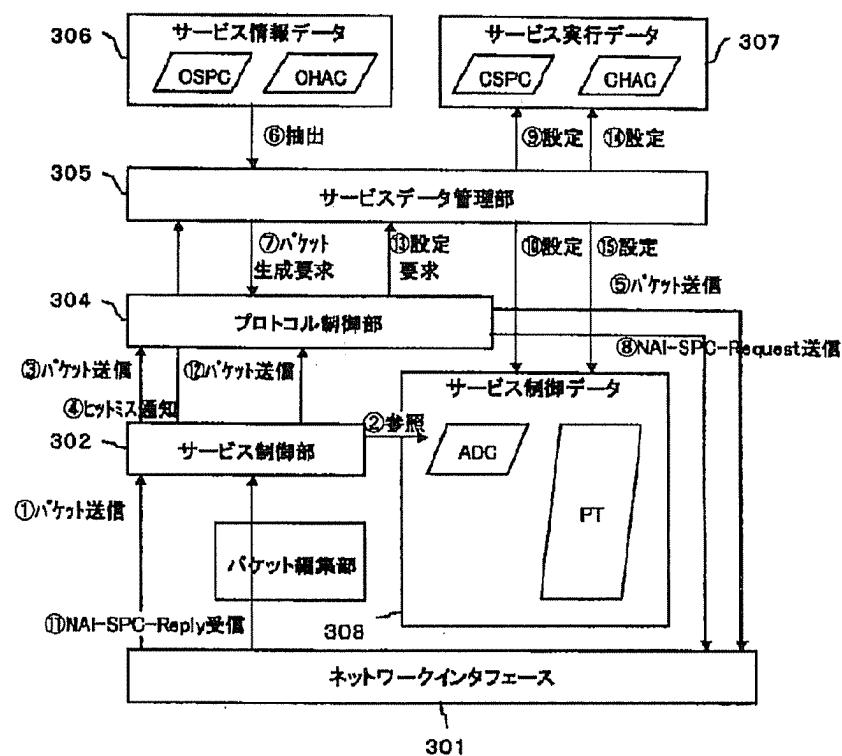
【図 6 4】

IPv6ヘッダの構成を示す図



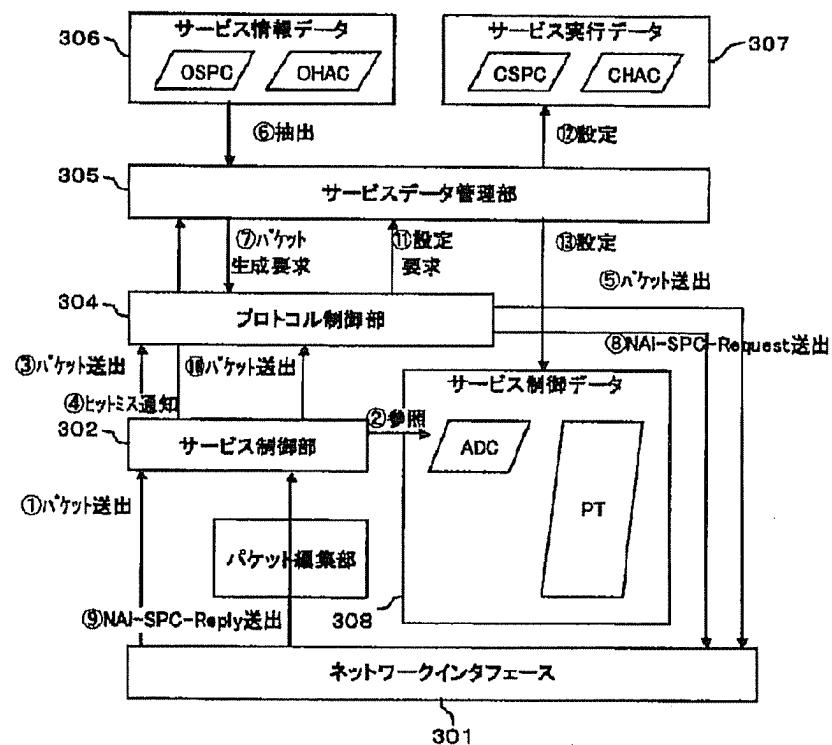
【図57】

送信側ヒットミスおよび受信側ヒットミスが発生した際の  
有効化処理のシーケンスを示す図



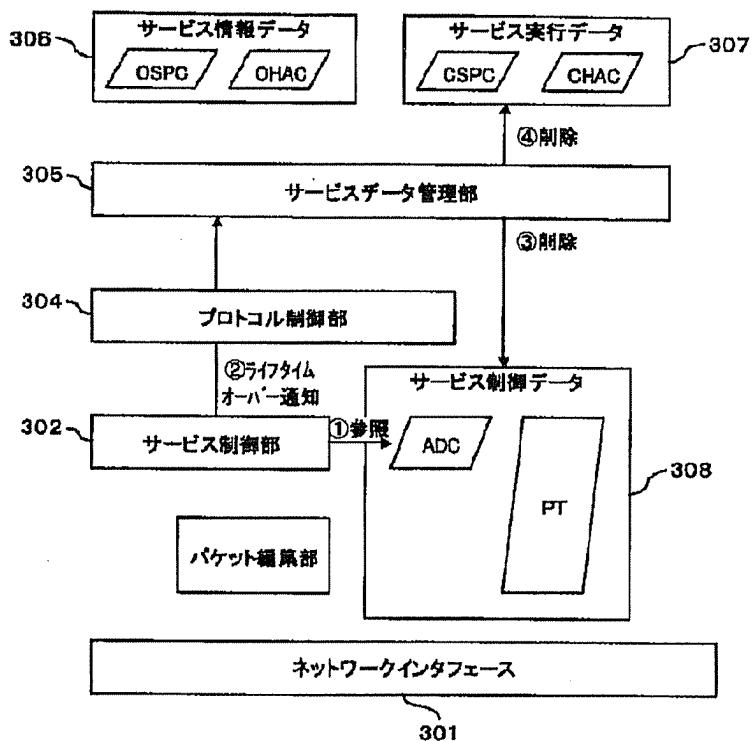
【図58】

送信側アドレスおよび受信側アドレスの組合せが  
登録されている場合の有効化処理のシーケンス



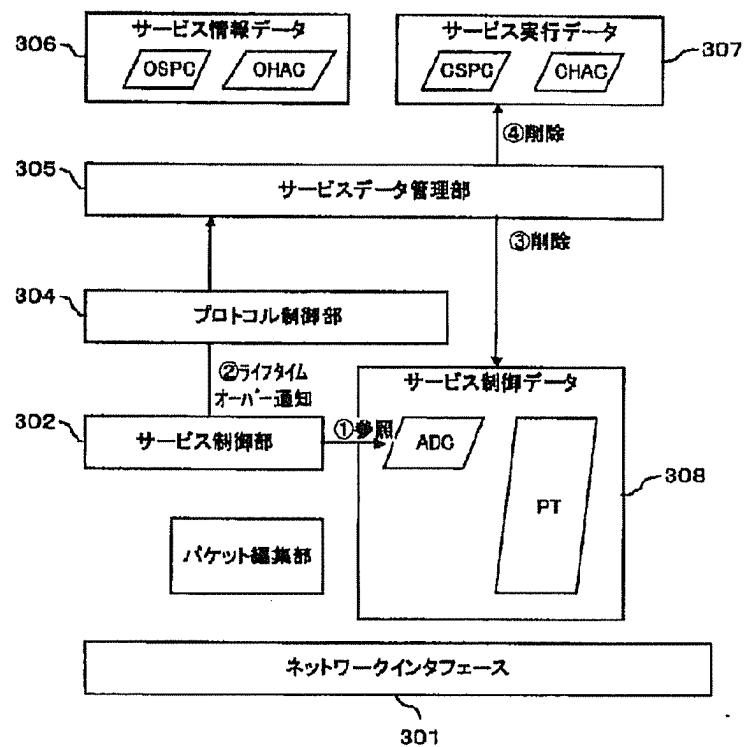
【図59】

送信側アドレスのライフタイムが消滅した場合の  
無効化処理のシーケンスを示す図



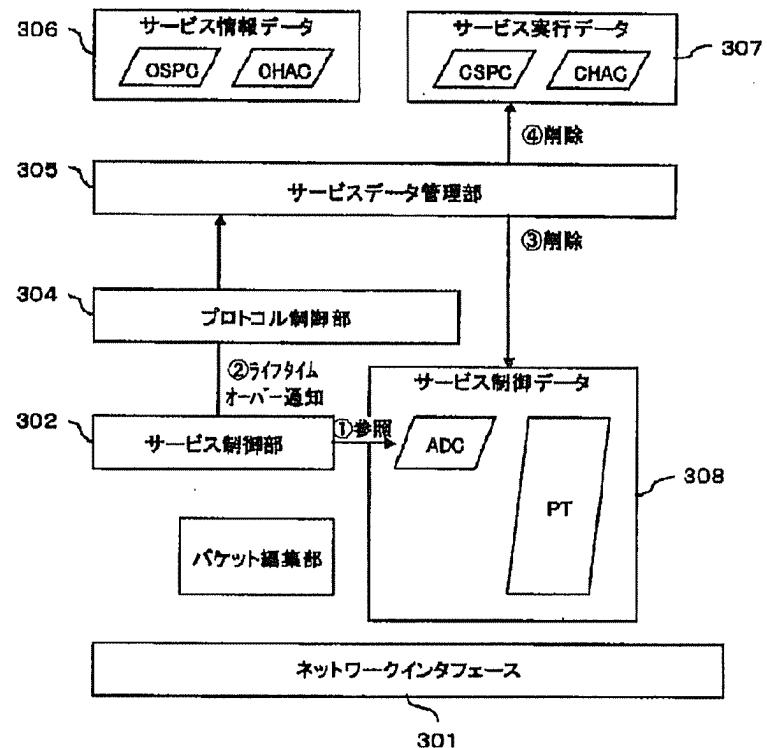
【図60】

受信側アドレスのライフタイムが消滅した場合の  
無効化処理のシーケンスを示す図



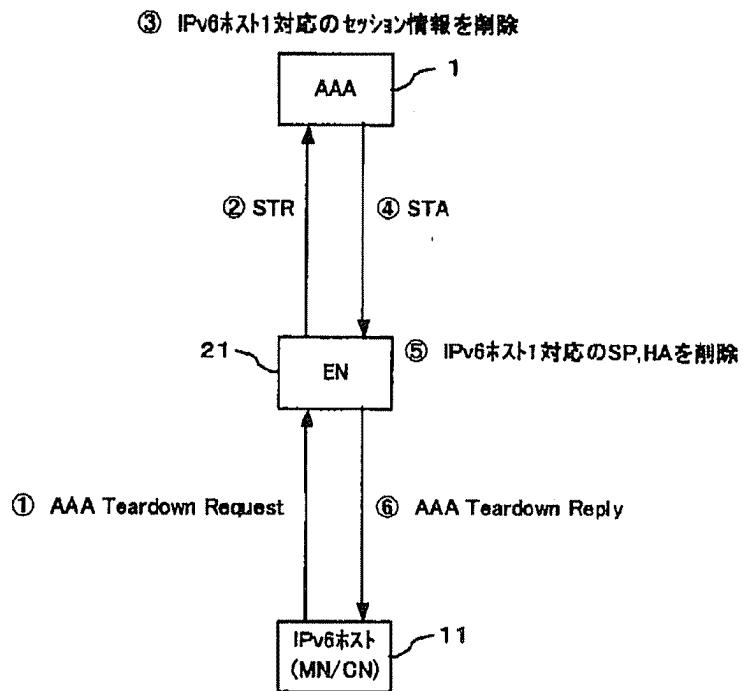
【図61】

送信側アドレスおよび受信側アドレスの組合せが登録されている場合の無効化処理のシーケンス



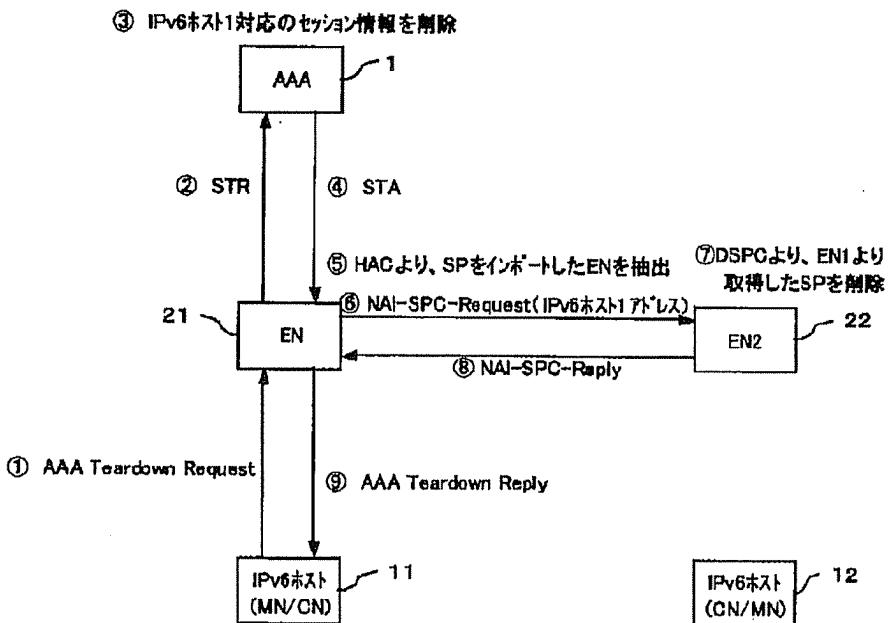
【図62】

IPv6ホストからの要求により  
サービスを無効化するシーケンスを示す図



【図63】

IPv6ホストからの要求により他のノードの  
サービス情報を削除／無効化するシーケンスを示す図



【図69】

(a) および (b) は、それぞれ、ASRメッセージおよび  
ASAメッセージのデータ構成を示す図

ASR

```

<AA-Service-Request> ::= < Diameter Header: XXX >
  < Session-Id >
  { Session-Timeout }
  { Authorization-Lifetime }

```

(a)

ASA

```

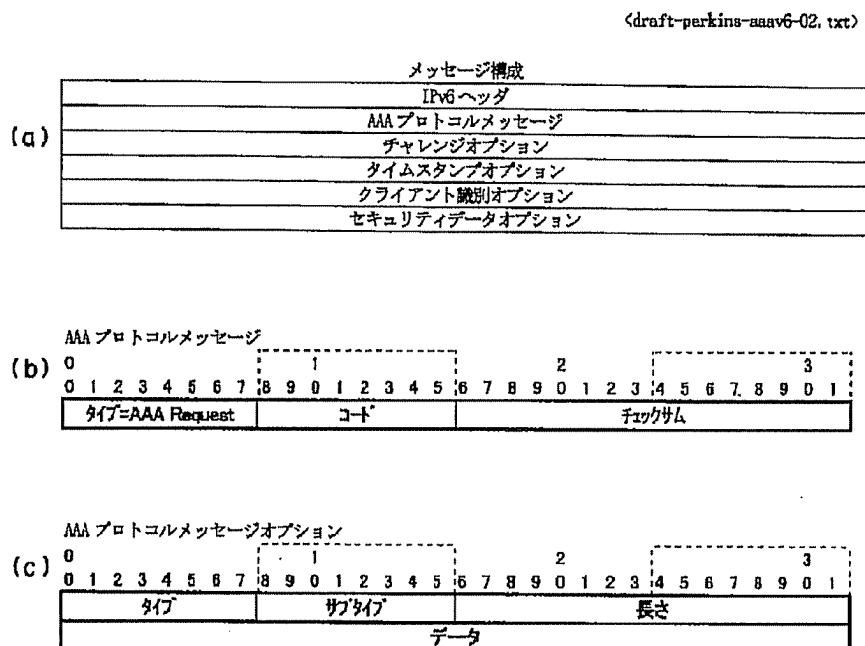
<AA-Service-Answer> ::= < Diameter Header: XXX >
  < Session-Id >
  { Session-Timeout }
  { Authorization-Lifetime }
  { Result-Code }
  { Profile-Cache AVP }

```

(b)

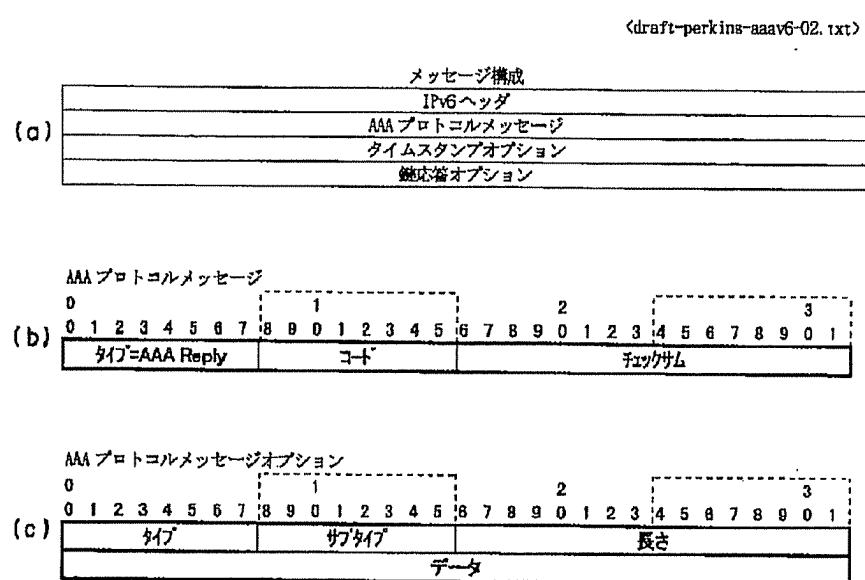
【図 6 5】

## ICMP-AAA 要求メッセージの構成を示す図



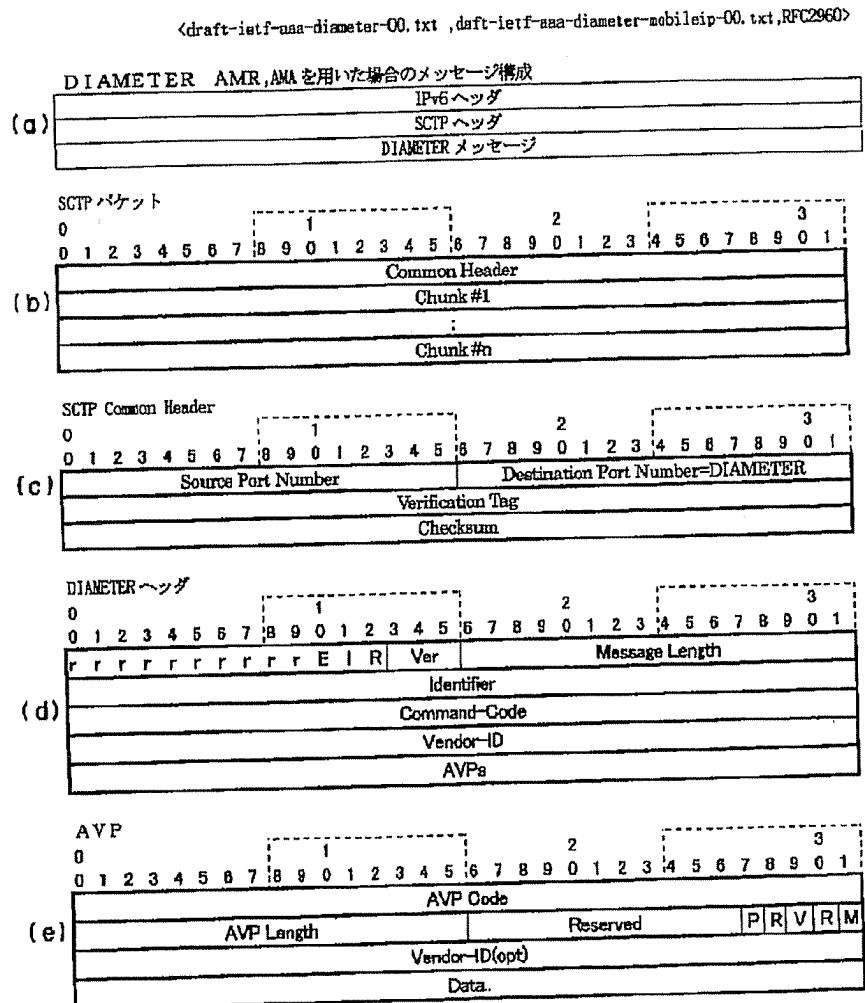
【図 6 6】

## ICMP-AAA 応答メッセージの構成を示す図



【図67】

DIAMETER メッセージを伝送するパケットの構成を示す図



【图68】

(a) および (b) は、それぞれ、AHR(AMR)メッセージ  
および AHA(AMA)メッセージのデータ構成を示す図

(a) **AAH(AMR)**

<AA-Mobile-Node-Request> ::= < Diameter Header: 260 >  
 { Session-ID }  
 { User-Name }  
 { Host-Name }  
 { Authorization-Lifetime }  
 { ICMP-AAA-Request }  
 {Timestamp}  
 {NAJ}  
 {認証データ}

(b) **AAIA(ANA)**

<AA-Mobile-Node-Answer> ::= < Diameter Header: 261 >  
 < Session-Id >  
 { Session-Timeout }  
 { Authorization-Lifetime }  
 { Result-Code }  
 { Host-Name }  
 { ICMP-AAA-Reply }  
 {Timestamp}  
 {認証データ}  
 {Profile-Cache AVP}

[図73]

## 結合更新メッセージのデータ構成を説明する

<draft-ietf-mobileip-hmipv6-01.txt>

### メッセージ構成

## IPv6 ヘッダ

## BLオプション

メッセージ構成	
(a)	IPv6 ヘッダ
	BU オプション

### BUオプション

0	1	2	3
0 1 2 3 4 5 8 7	8 9 0 1 2 3 4 5	6 7 8 9 0 1 2 3	4 5 6 7 8 9 0 1
Option Type			
Option Length			
A   H   R   D   M   B   Res	Prefix Length	Sequence Number	
Lifetime			
Sub-Options...			

## 【図70】

(a)～(d)は、それぞれ、HHRメッセージ、HHAメッセージ、STRメッセージ、STAメッセージのデータ構成を示す図

```

HHR
<AA-Service-Request> ::= < Diameter Header: 262 >
  < Session-Id >
  { Session-Timeout }
  { Authorization-Lifetime }
  { Profile-Cache AVP }
  //////////////

HHA
<AA-Service-Request> ::= < Diameter Header: 263 >
  < Session-Id >
  { Session-Timeout }
  { Authorization-Lifetime }
  { Result-Code }

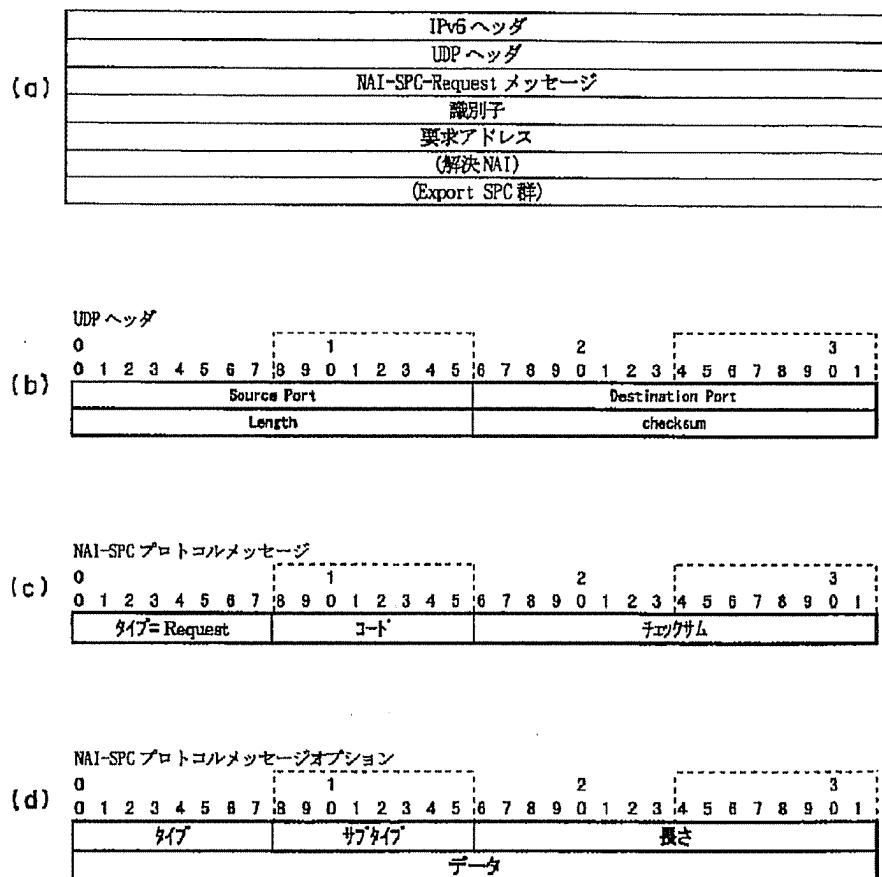
STR
<Session-Termination-Request> ::= < Diameter Header: 275 >
  < Session-Id >
  { Host-Name }
  { User-Name }

STA
<Session-Termination-Answer> ::= < Diameter Header: 276 >
  < Session-Id >
  { Result-Code }
  { Host-Name }
  { User-Name }

```

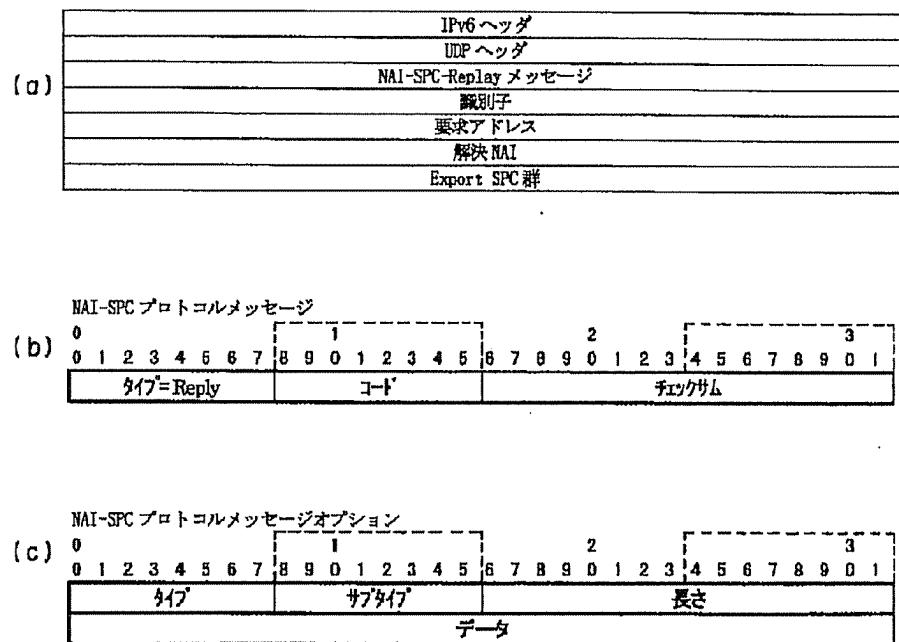
【図71】

## NAI-SPC要求メッセージのデータ構成を説明する図



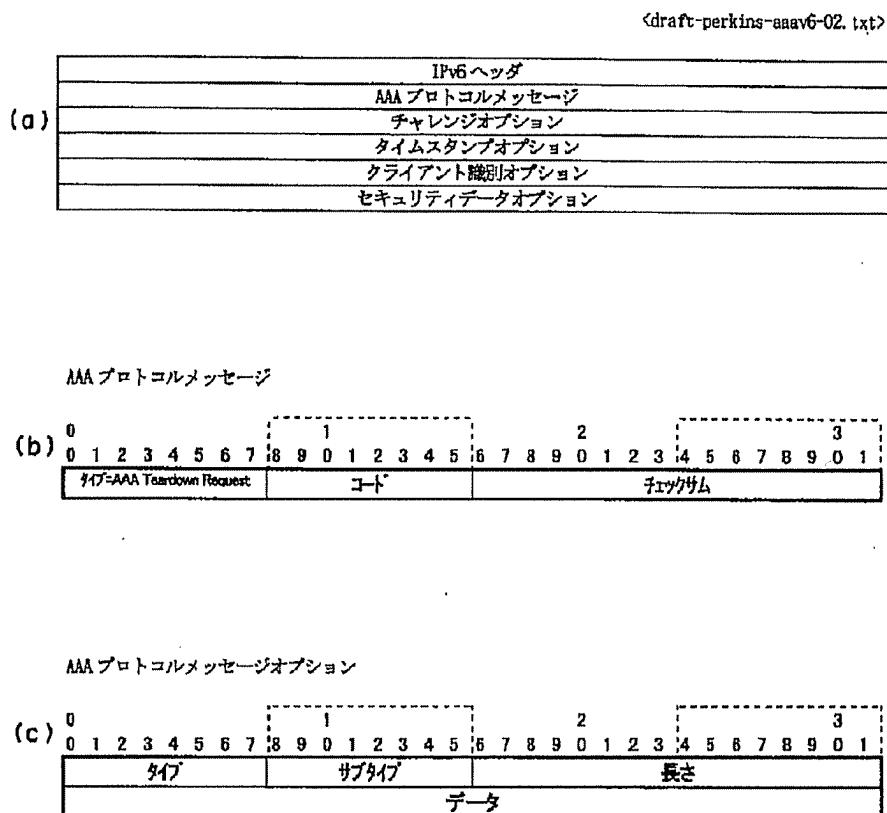
【図72】

## NAI-SPC 応答メッセージのデータ構成を示す図



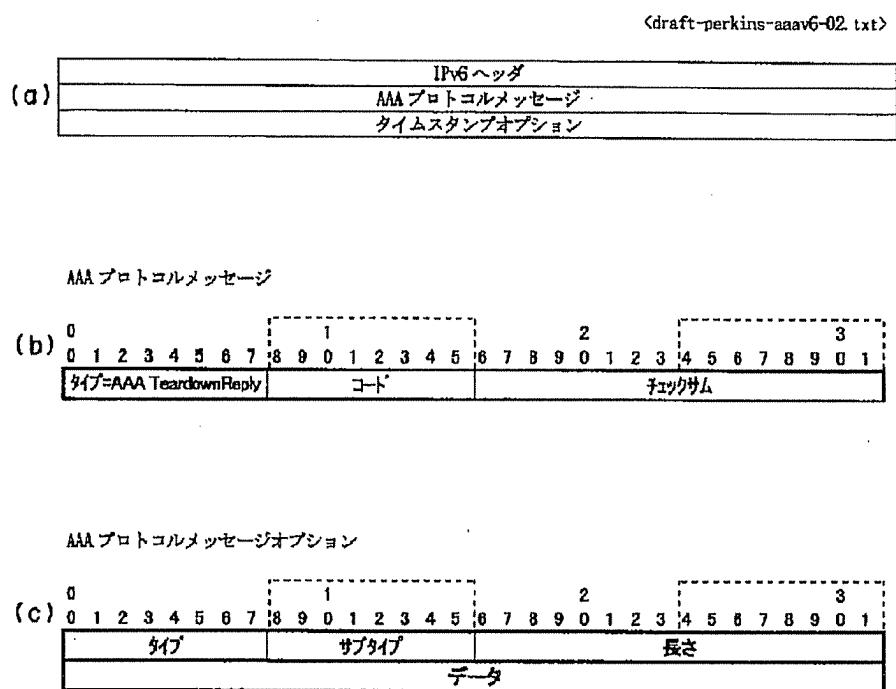
【図74】

ICMP-AAA-TearDown要求メッセージのデータ構成を説明する図



【図75】

## ICMP-AAA-TearDown応答メッセージのデータ構成を説明する図




---

フロントページの続き

(72)発明者 村田 一徳

福岡県福岡市早良区百道浜2丁目2番1号

富士通西日本コミュニケーション・シス

テムズ株式会社内

(72)発明者 岩本 勝徳

福岡県福岡市早良区百道浜2丁目2番1号

富士通西日本コミュニケーション・シス

テムズ株式会社内

(72)発明者 山村 新也

福岡県福岡市早良区百道浜2丁目2番1号

富士通西日本コミュニケーション・シス

テムズ株式会社内

(72)発明者 五十嵐 洋一郎

神奈川県川崎市中原区上小田中4丁目1番

1号 富士通株式会社内

(72)発明者 若本 雅晶

神奈川県川崎市中原区上小田中4丁目1番

1号 富士通株式会社内

Fターム (参考) 5B089 GA11 GA31 HA10 HB10 JA35

JB10 JB15 KA13 KB06 KB11

5K030 GA10 GA19 HA08 HB08 HD03

KA06